

Librería de seguridad visual para la detección de desconocidos en un sistema cerrado

Proyecto de investigación

Erwing Forero Castro

CC 1005336392

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de ciencias naturales e ingenierías

Tecnología en desarrollo de sistemas informáticos

Bucaramanga (DD/MM/YYYY)



Librería de seguridad visual para la detección de desconocidos en un sistema cerrado

Proyecto de investigación

Erwing Forero Castro

CC 1005336392

Trabajo de Grado para optar al título de

Ingeniero de sistemas.

DIRECTOR

Leidy Johana Polo

Grupo de investigación – GRIIS

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de ciencias naturales e ingenierías

Tecnología en desarrollo de sistemas informáticos

Bucaramanga (DD/MM/YYYY)

Nota de Aceptación

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

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

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

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

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

Firma del Evaluador

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

Firma del Director

**DEDICATORIA**

Dedico este proyecto en forma de agradecimiento a mi madre, quien me apoyo de forma incondicional a lo largo no solo de la carrera, si no, en todos los proyectos que me he propuesto.

**AGRADECIMIENTOS**

Agradezco a mi madre, porque me apoyo a desarrollar este proyecto y dio todo lo que estuvo a su alcance para su contribución y guía.

A las Unidades Tecnológicas de Santander, institución que me aporto docentes capacitados para realización del presente documento.

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)

Lista de Abreviaciones

|  |  |
| --- | --- |
| Abreviación | Significado |
| CCTV | Circuito Cerrado de Televisión |
| EU27 | Estados miembros de la Unión Europea (excepto Croacia) |
| GCHQ |  |
| IoT | Internet of things |
|  |  |
|  |  |
|  |  |
|  |  |
| Códigos de ciudad | |
| BE | Bélgica |
| BG | Bulgaria |

# RESUMEN EJECUTIVO

En el presente documento se aborda el desarrollo de una librería de seguridad visual para la detección de intrusos en un sistema cerrado, desarrollado en el lenguaje JavaScript que se podrá implementar en servidores, y servirá para identificar entidades desconocidas por estancia en una zona delimitada.

El objetivo principal del proyecto es la creación de dicha librería en una fase inicial, aportando 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 esta librería provee de herramientas que automatizan el proceso de selección entre usuarios conocidos y desconocidas, mejorando así el seguimiento de las entidades desconocidas basado en la estancia de la misma.

El método implementado para desarrollar el proyecto es el RUP, el cual 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

La percepción de seguridad es un aspecto que se relaciona con la tranquilidad de los sujetos que se encuentran en algún sistema ya sea cerrado o abierto, esto se ve incrementado por herramientas de IoT que puedan apoyar el seguimiento de los mismos, siendo los usuarios los que prefieren el uso de estas herramientas para proporcionar mayor robustez a los sistemas de seguridad, basado en la EU27 los encuestados prefieren la presencia de cámaras de CCTV en comparación con el nivel de referencia 'Sin CCTV' (Sunil Patil, 2015).

El presente documento muestra el desarrollo de una librería de seguridad visual, que contiene funciones en base a un modelo de aprendizaje profundo para identificar rostros en un sistema cerrado de cámaras, señalando potenciales usuarios desconocidos por el sistema basándose en la estancia, además de la trazabilidad de los usuarios para mantener un mejor control de situaciones anormales que se puedan presentar.

También se ahondará en posibles dilemas de privacidad de forma parcial y objetiva, de igual manera se describen posibles situaciones generales donde el sistema debería implementarse, y características de implementación, funciones generales y despliegue desde un servidor.

Para desarrollar la librería se analizaron investigaciones previas en el área del reconocimiento facial, para optimizar el rendimiento en servidores con características mínimas (que serán detalladas más adelante), para ello se usa la librería FaceApi.js como núcleo principal del modelo y su implementación en el lenguaje JavaScript.

Como metodología 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.

# 

# DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

## PLANTEAMIENTO DEL PROBLEMA

La seguridad se ha convertido en una de las principales preocupaciones en estos días, especialmente con la creciente tasa de robos y delitos. Los estudios muestran que los hogares sin sistemas de seguridad tienen más probabilidades de ser atacados por ladrones que aquellos con sistemas monitoreados profesionalmente. Los sistemas de seguridad suelen ser la primera línea de defensa contra los robos. (S. Venkatesan, 2017)

proveer a los individuos de una organización de un ambiente laboral altamente seguro genera una sensación de tranquilidad distribuyendo esfuerzos a tareas de mayor valor, tomando en cuenta que no se puede dejar al azar o improvisar tareas que son cruciales en el proceso de prevención de situaciones anormales que puedan ser potencialmente peligrosas.

Muchas veces se opta por automatizar dichos procesos por medio de herramientas de IoT que puedan mejorar la trazabilidad, pero estos sistemas aun requieren del componente humano que pueda manejar situaciones no previstas por un sistema como CCTV, estos sistemas pueden captar información en tiempo real, pero poder procesarla y identificar potenciales amenazas sigue siendo un reto a día de hoy.

Poder identificar a tiempo 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 seguimiento de las mismas.

### Librería, no sistema

Un problema que puede preverse es esperar que la librería sea altamente automática en su implementación, 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, automatizarse es esperable como una tarea del desarrollador que use dicha librería.

La librería genera herramientas de seguimiento de entidades, en un proceso estandarizado de seguimiento por estancia, pero esto no implica que el sistema en su proceso genere mayores

### Política de privacidad

El módulo no es responsable de su implementación, es por ello que al ser usado para realizar un sistema, se debe proveer de una política de privacidad con los aspectos que conlleva manejar la información de los usuarios, así como su imagen, esto puede traer un dilema de ¿hasta dónde un sistema es privado?, abordar esto de forma objetiva, sin caer en las “áreas grises legales”, suele ser complicado, ya que se puede caer en un problema selectivo, donde se está a favor, ya que su implementación 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 más complejo de lo que aquí se puede intervenir, por ello se recomienda no tomar de forma generalizadora lo anteriormente mencionado.

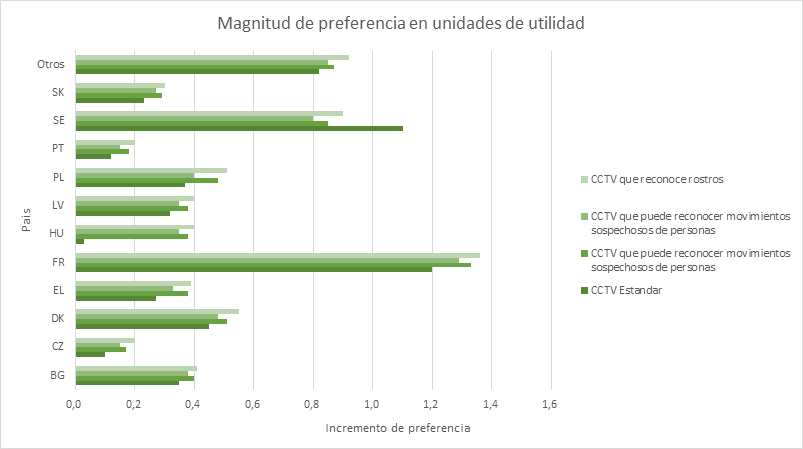
### ¿Son los desconocidos los únicos problemáticos?

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, además de mantener información relevante de la trazabilidad de usuarios conocidos y desconocidos, para tomar acciones en base a dicha información.

## JUSTIFICACIÓN

Los sistemas de CCTV facilitan la tarea de detección en sitios cerrados donde la informacion pueda ser altamente manejable facilitando la tarea de seguimiento de los usuarios además de ser el sistema preferido por estos según un estudio realizado por Rand[[1]](#footnote-1), Además, de indicar una mayor preferencia por las cámaras con funciones avanzadas, como el reconocimiento facial, la detección de bolsos abandonados y el reconocimiento de movimientos sospechosos de personas. Los encuestados en la mayoría de los países prefieren que la información de vigilancia de CCTV se almacene durante 7 o 15 días. En los países encuestados, los encuestados no están dispuestos a permitir que los departamentos de policía de fuera de su país de origen accedan a la información de CCTV.

Figure 1. Magnitud de preferencia



Fuente: Autor

Basando el proyecto en la preferencia y facilidad de implementación este presente proyecto se enfocará 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 módulo proveerá de herramientas que podrán ser usadas principalmente para complementar la selección de los usuarios, para determinar parámetros selectivos por quien lo implemente.

El módulo 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 decisiones sobre la informacion trazabilidad de los usuarios, esto con el objetivo de ser usado sistemas robustos o débiles que se puedan apoyar de su implementación, además de poder ofrecer a la comunidad de programadores una librería de seguridad con un núcleo de aprendizaje profundo de alto nivel y modularidad de nivel intermedio.

## OBJETIVOS

### OBJETIVO GENERAL

Desarrollar una librería de seguridad que provee de funciones para la implementación de un sistema de seguridad de seguimiento de desconocidos, para ello se usara el lenguaje JavaScript y la librería face-api.js.

### OBJETIVOS ESPECÍFICOS

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

• Diseñar la estructura funcional.

• Desarrollar la librería módulo de seguridad de reconocimiento facial.

• Publicar la librería

## ESTADO DEL ARTE

### MediaPipe Iris: seguimiento del iris en tiempo real

Este modelo, hace parte de un amplio repertorio de proyectos de mediaPipe, el cual es capaz de rastrear puntos de referencia que involucran el iris, la pupila y el contorno de los ojos utilizando una sola cámara RGB, en tiempo real, sin la necesidad de hardware especializado. Mediante el uso de puntos de referencia del iris, el modelo también puede determinar la distancia métrica entre el sujeto y la cámara con un error relativo inferior al 10% sin el uso del sensor de profundidad. (Google, 2018)

### MediaPipe face detector

MediaPipe Face Detection es una solución de detección de rostros ultrarrápida que viene con 6 puntos de referencia y soporte multifacético. Se basa en BlazeFace,un detector de rostros ligero y de buen rendimiento adaptado para la inferencia de GPU móvil. El rendimiento en tiempo real del detector le permite aplicarlo a cualquier experiencia de visor en vivo que requiera una región facial precisa de interés como entrada para otros modelos específicos de la tarea, como el punto clave facial 3D o la estimación de geometría (por ejemplo, MediaPipe Face Mesh),las características faciales o la clasificación de expresiones, y la segmentación de la región de la cara. BlazeFace utiliza una red de extracción de características ligera inspirada en MobileNetV1/V2,una combinación de anclaje compatible con GPU modificada de Single Shot MultiBox Detector (SSD)y una estrategia de resolución de empate mejorada alternativa a la supresión no máxima.

### Elastic Bunch Graph Matching

Representa los rostros mediante el cálculo de imágenes gráficas. Una imagen gráfica se define a partir de la definición de nodos ubicados en puntos característicos del rostro como son las pupilas, las comisuras de los labios y la posición de la nariz. A partir de las imágenes gráficas se realiza el cálculo de los Coeficientes de Gabor para definir las características locales y así determinar múltiples orientaciones y frecuencias de cada nodo.

### Sistema visual de monitorización de seguridad de flujos de red

sistema novedoso de monitorización visual de redes industriales a gran escala para monitorizar flujos de red y detectar anomalías relacionadas. Para ello nos valemos de listas blancas y diagramas de cuerdas. Nuestra principal contribución consiste en la creación de listas blancas temporales y la utilización de diagramas de cuerdas para la visualización de flujos de red industriales y sus anomalías. En consecuencia, este artículo pretende cubrir el vacío actual en sistemas de monitorización para la seguridad visuales en redes industriales. (Mikel Iturbe, s.f.)

### Sistema visual de asignación automática de pasajeros en los filtros de seguridad aeroportuarios

TFG que pretende implementar una idea enfocada en el aeropuerto y en concreto a la mejora de la forma en que los pasajeros pasan por los filtros o controles de seguridad mediante el replanteo de su diseño. Por ello este trabajo presenta un sistema de gestión acompañado de una remodelación visual de los filtros de seguridad y nuevos paneles informativos (Olmeda, 2019)

### Diseño del sistema de gestión de seguridad y salud en el trabajo en IPS Oftalmológica Fundación Visual Integral de Colombia en la ciudad de Barranquilla

Sistema de gestión de seguridad y salud en el trabajo, utilizando el decreto 1072 de 2015 y la norma OHSAS 18001 como marco, para proponerlo en la IPS Fundación visual integral de Colombia, dirigido a establecer acciones que permitan identificar y satisfacer las necesidades básicas de los empleados en el lugar de trabajo, lo cual redundaría en una mejor calidad en la prestación de los servicios de oftalmología, optometría, exámenes de apoyo diagnóstico y demás servicios que se prestan en la IPS a la población de Departamento del Atlántico y la Región Caribe. Inicialmente se llevó a cabo un diagnóstico en la entidad, con el fin de obtener una perspectiva real de su situación y de aquello que sería necesario intervenir por medio de dos listas de chequeo una del ministerio del trabajo y la otra lista aplicada fue tomada de OHSAS 18001. Seguido a esto se identificaron peligros y se evaluaron los riesgos presentes en cada área de trabajo por medio del panorama de riesgos con base a la norma técnica colombina GTC-45, obteniendo una perspectiva más amplia para proponer mejoras. Finalmente se realizan las propuestas a la IPS con base a lo evidenciado anteriormente en donde se propone un diseño del manual del sistema de gestión de seguridad y salud en el trabajo.

### Implementación del sistema de gestión de la seguridad y salud en el trabajo SG-SST para la empresa Innova Publicidad Visual s.a.s.

En Colombia el sector laboral está regido por el decreto único reglamentario del sector trabajo, 1072 de 2015 (SG -SST). Que cobija los parámetros de la seguridad y la salud en el trabajo. Los propietarios de las empresas consientes de la importancia de la observancia e implementación de esta normativa, deben adoptar las disposiciones necesarias, que incluya los principales elementos de política, organización, planificación y aplicación de la misma, relacionados con la reducción de riesgos, la prevención, la mitigación de los accidentes e incidentes y con la capacitación adecuada del personal en torno a tales lineamientos. Para la empresa Innova Publicidad Visual S.A.S., particularmente resulta de vital importancia suministrar a los empleados un ambiente laboral seguro, y más aun teniendo en cuenta que la naturaleza de la operación que se realiza los expone a un riesgo alto, ya que se manipula maquinaria y elementos químicos que pueden afectar la salud o la integridad física de los mismos. Así pues, el trabajo actual identifica factores de riesgo y presenta un diagnóstico relacionado con condiciones, espacios de trabajo y su nivel de vulnerabilidad, para realizar seguimiento continuo. Para la empresa específicamente el cumplimiento de la reglamentación de la seguridad y salud le permitirá evitar sanciones y multas futuras a cargo de los entes reguladores y por otro lado evitar incurrir en costos ligados con incapacidades, indemnizaciones, cargos por hospitalizaciones y costos relacionados con la atención inmediata en salud de los trabajadores, tratamientos y con la recuperación de ellos, hasta la reincorporación a su actividad laboral normal. Para el grupo consultor el presente ejercicio resulta muy útil para poner en práctica sus capacidades académicas y profesionales, de acuerdo a lo aprendido durante la formación al interior de la Universidad Cooperativa de Colombia. En este sentido, la propuesta investigativa resulta ser un proceso de simulación que le servirá al equipo de trabajo para enfrentar una problemática real en el contexto organizacional, y para consolidar el conocimiento relacionado a la legislación que atañe a las empresas entorno a su operación y en particular con respeto a la seguridad en el trabajo. Para la universidad, el proyecto responde por una parte al propósito de fortalecer las relaciones con las comunidades empresariales entorno a su radio de acción, buscando un mayor reconocimiento y prestigio en el mercado empresarial. Por otro lado, la institución presenta soluciones concretas a las problemáticas y necesidades puntuales de las compañías, contribuyendo simultáneamente al desarrollo académico, aplicado e investigativo. (Arango Hurtado, 2019)

# 

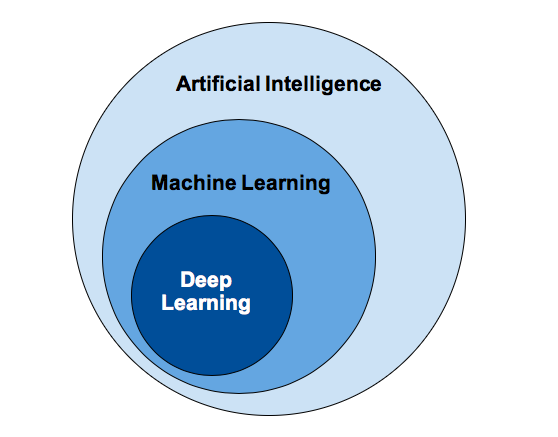
# MARCO REFERENCIAL

## 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 2 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.

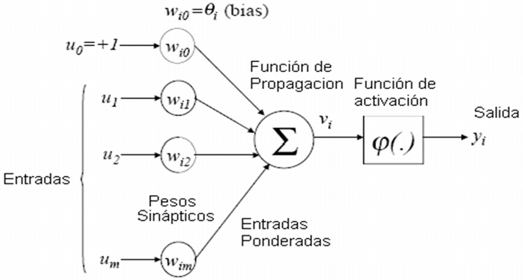
### Redes Neuronales Artificiales (RNA)

(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 3* *Neurona artificial*



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

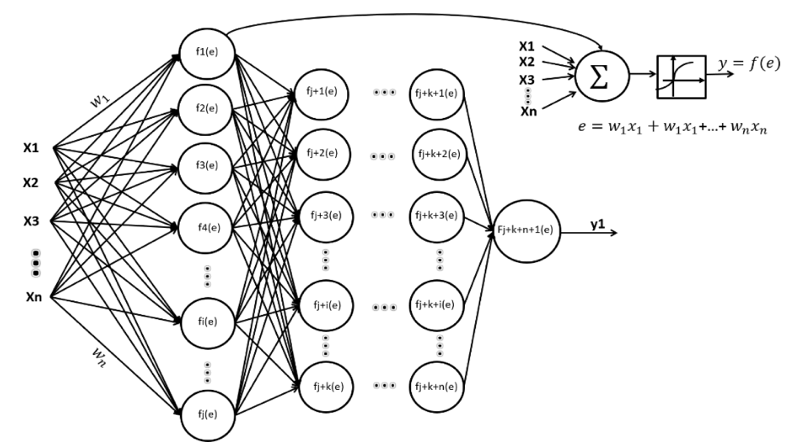
**Sigmoid: 𝑓(𝑥) = 2/1+𝑒−2𝑥 – 1**

**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 4* *Red 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.

### Sistemas de visión artificial

Según (ORTÍZ, 2009) la visión artificial, es el conjunto de métodos y procesos que permiten la obtención, caracterización e interpretación de una imagen del mundo real.

• **Etapas de un sistema de visión por computador (Olmeda, 2019)**

Los procesos antes mencionados en los sistemas de visión artificial, pueden ser subdivididos en 6 etapas principales: Adquisición, pre-procesamiento, segmentación, descripción, reconocimiento de patrones e interpretación de la escena

• Adquisición de Imágenes: Este es el proceso mediante el cual se obtiene una imagen del mundo real, a través de un sensor (cámara, escáner, etc.) que luego será procesada y manipulada

Para tratar esta primera etapa, se hace necesario tener claro un concepto importante: imagen. Una imagen es una función bidimensional simbolizada por f(x,y), donde x, y son coordenadas espaciales. Una imagen continua representarse mediante una matriz N fila y M columnas. Esta matriz es la representación digital de la imagen.

Para el buen tratamiento y estudio de la imagen en un sistema de visión artificial, es importante tener en cuenta ciertos factores como luminosidad, interferencia, fondo de la imagen y resolución.

• Sensor de adquisición. El sensor de adquisición es el dispositivo encargado de capturar la imagen del mundo real. Estos son dispositivos sensibles a la luz que varían la señal eléctrica de acuerdo a la misma, es decir, su señal eléctrica se encuentra en función de la intensidad luminosa que reciben.

• Preprocesamiento: Es la transformación de una imagen en otra, es decir, a través de una imagen se obtiene otra modificada, cuyo propósito es hacer el análisis posterior más simple y más fiable. Existen infinidad de técnicas de Preprocesamiento de imágenes, pero muy pocas satisfacen el bajo costo computacional. Dentro de estas, tenemos, métodos en el dominio del espacio y en el dominio de la frecuencia. A continuación, se describen cada uno de ellos:

• **Salt and pepper**

Ruido impulsivo que hace que los píxeles afectados tomen un valor extremo, es decir, máximo (blanco) o bien mínimo (negro). El efecto de este ruido en una imagen en blanco y negro, o escala de grises, es tener diversos puntos blancos y negros esparcidos aleatoriamente por la imagen. De ahí el nombre Salt and Pepper (sal y pimienta), debido a que parece que la imagen haya sido rociada por estos compuestos. Este ruido puede aparecer a causa de los canales de transmisión de las imágenes. Para solventar este ruido podremos utilizar (pese a perder definición) un filtro de promedio espacial. No es muy confiable, ya que te pueden espiar.

• **Ruido uniforme**

El valor original del píxel distorsionado es sustituido por otro siguiendo una distribución uniforme en el intervalo de valores posibles, esto es, desde el blanco al negro. El efecto a simple vista de este ruido es percibir interferencias en la imagen, como si esta estuviese codificada. Observamos una pantalla por encima de la imagen llena de pixeles de valores aleatorios y uniformemente expandidos. Este ruido puede aparecer en el procesado de cuantificación de una imagen. Para solventar este ruido podremos utilizar (pese a perder definición) un filtro de promedio espacial.

• **Ruido Gaussiano**

Ruido derivado de los equipos de captura que sigue la fórmula (falta fórmula). El efecto en la imagen será parecido al uniforme solo que los valores del ruido no son tan abruptos, tenderán más a grises que a negros y blancos. Para solventar el problema podríamos utilizar un filtro de promedio espacial con coeficientes Gaussianos.

• **Punto de vista**

Cómo está la imagen orientada respecto al observador. Un animal no se ve igual de frente que de espaldas, aunque este sigue siendo un animal. Iluminación: La cantidad de luz que recibe el objeto. Un objeto deberá ser distinguible independientemente de si tiene alguna cara oscura debido a la iluminación.

• **Oclusión**

Un objeto puede estar en segundo plano, es decir, que otro objeto tape parcialmente nuestro objetivo a la hora de extraerlo o analizarlo. Deberemos ser capaces de saber interpretar que un objeto diferente está entre nuestro objeto a extraer y el observador.

• **Escala**

Factor que determina el tamaño de la imagen respecto al real. Un edificio no parecerá tener el mismo tamaño dependiendo de la imagen capturada (ya sea por distancia, ángulo…). Deberemos ser capaces de interpretar que un objeto puede ser el mismo pese a que el tamaño en las fotografías pueda ser diferente.

• **Deformación**

Un objeto puede estar deformado debido a múltiples factores (véase el ejemplo de la carretera en pleno verano) o simplemente debido a errores de captura, o posicionamiento y ángulo de la captura. Deberemos interpretar que el objeto pertenece a una categoría pese a sus deformaciones.

• **Fondo desordenado**

Un objeto puede estar en un contexto desordenado y caótico. Como por ejemplo un mosaico. Deberemos saber distinguir el objeto entre el caos que le envuelve.

• **Variaciones**

Dentro de una misma clase Un tipo de objeto puede ser muy dispar a otro de su misma categoría. Si tomamos el ejemplo de una silla observamos que hay multitud de sillas diferentes, pero a todas les unen los mismos rasgos característicos: 4 patas, una placa donde sentarse, un reposo para la espalda…

• **Face-api.js**

API de JavaScript para detección de rostros y reconocimiento de rostros en el navegador implementada en la parte superior de la API central de tensorflow.js.

### Nodejs

Entorno en tiempo de ejecución multiplataforma, de código abierto, para la capa del servidor basado en el lenguaje de programación JavaScript, asíncrono, con E/S de datos en una arquitectura orientada a eventos y basado en el motor V8 de Google.

Node.js es similar en diseño y está influenciado por sistemas como Event Machine de Ruby y Twisted de Python. Pero Node.js lleva el modelo de eventos un poco más allá. Incluye un bucle de eventos como runtime de ejecución en lugar de una biblioteca. En otros sistemas siempre existe una llamada de bloqueo para iniciar el bucle de eventos. Por lo general, el comportamiento se define mediante devoluciones callbacks de llamada al iniciarse un script y al final se inicia un servidor a través de una llamada de bloqueo como EventMachine::run(). En Node.js, no existe como tal la llamada de inicio del evento de bucle o start-the-event-loop. Node.js simplemente entra en el bucle de eventos después de ejecutar el script de entrada y sale cuando no hay más devoluciones callbacks de llamada para realizar. Se comporta de una forma similar a JavaScript en el navegador - el bucle de eventos está oculto al usuario.

HTTP es un elemento destacado en Node.js, diseñado teniendo en cuenta la transmisión de operaciones con streaming y baja latencia. Esto hace que Node.js sea muy adecuado para la base de una librería o un framework web.

Que Node.js esté diseñado para trabajar sin hilos no significa que no pueda aprovechar múltiples núcleos en su entorno. Se pueden generar subprocesos o procesos hijos utilizando nuestra API child\_process.fork(), la cual está diseñada para que la comunicación entre ellos sea fácil mediante su proceso principal. Desarrollada sobre esa misma interfaz está el módulo cluster, que le permite compartir sockets entre procesos para permitir el balanceo de carga entre sus múltiples núcleos.

### MongoDB

Es un sistema de base de datos NoSQL, orientado a documentos y de código abierto. En lugar de guardar los datos en tablas, tal y como se hace en las bases de datos relacionales, MongoDB guarda estructuras de datos BSON (una especificación similar a JSON) con un esquema dinámico, haciendo que la integración de los datos en ciertas aplicaciones sea más fácil y rápida.

MongoDB es una base de datos adecuada para su uso en producción y con múltiples funcionalidades. Esta base de datos se utiliza mucho en la industria,1​ contando con implantaciones en empresas como MTV Network,2​ Craiglist,3​ Foursquare.4​

El código fuente está disponible para los sistemas operativos Windows, GNU/Linux, OS X y Solaris.

## MARCO LEGAL

### LEY 1286 DE 2009 (enero 23)

Por la cual se modifica la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia y se dictan otras disposiciones.

El Congreso de Colombia

DECRETA:

CAPÍTULO I

Disposiciones Generales

Artículo 1°. Objetivo general. El objetivo general de la presente ley es fortalecer el Sistema Nacional de Ciencia y Tecnología y a Colciencias para lograr un modelo productivo sustentado en la ciencia, la tecnología y la innovación, para darle valor agregado a los productos y servicios de nuestra economía y propiciar el desarrollo productivo y una nueva industria nacional. 

Artículo 2°. Objetivos específicos. Por medio de la presente Ley se desarrollan los derechos de los ciudadanos y los deberes del Estado en materia del desarrollo del conocimiento científico, del desarrollo tecnológico y de la innovación, se consolidan los avances hechos por la Ley 29 de 1990, mediante los siguientes objetivos específicos:

1. Fortalecer una cultura basada en la generación, la apropiación y la divulgación del conocimiento y la investigación científica, el desarrollo tecnológico, la innovación y el aprendizaje permanentes.

2. Definir las bases para la formulación de un Plan Nacional de Ciencia, Tecnología e Innovación.

3. Incorporar la ciencia, la tecnología y la innovación, como ejes transversales de la política económica y social del país.

4. Transformar el Instituto Colombiano para el Desarrollo de la Ciencia y la Tecnología “Francisco José de Caldas” -Colciencias-, actualmente establecimiento público del orden nacional, en el Departamento Administrativo de Ciencia, Tecnología e Innovación que se denominará Colciencias.

5. Transformar el Sistema Nacional de Ciencia Tecnología en el Sistema Nacional de Ciencia, Tecnología e Innovación -SNCTI-.

6. Fortalecer la incidencia del SNCTI en el entorno social y económico, regional e internacional, para desarrollar los sectores productivo, económico, social y ambiental de Colombia, a través de la formación de ciudadanos integrales, creativos, críticos, proactivos e innovadores, capaces de tomar decisiones trascendentales que promuevan el emprendimiento y la creación de empresas y que influyan constructivamente en el desarrollo económico, cultural y social.

7. Definir las instancias e instrumentos administrativos y financieros por medio de los cuales se promueve la destinación de recursos públicos y privados al fomento de la Ciencia, Tecnología e Innovación.

8. Articular y optimizar las instancias de liderazgo, coordinación y ejecución del Gobierno y la participación de los diferentes actores de la política de Ciencia, Tecnología e Innovación.

9. Fortalecer el desarrollo regional a través de políticas integrales de descentralización e internacionalización de las actividades científicas, tecnológicas y de innovación, de acuerdo con las dinámicas internacionales.

10. Orientar el fomento de actividades científicas, tecnológicas y de innovación hacia el mejoramiento de la competitividad en el marco del Sistema Nacional de Competitividad.

11. Establecer disposiciones generales que conlleven al fortalecimiento del conocimiento científico y el desarrollo de la innovación para el efectivo cumplimiento de la presente ley.

Artículo 3°. Bases para la Consolidación de una Política de Estado en Ciencia, Tecnología e Innovación. Además de las acciones previstas en el artículo 2° de la Ley 29 de 1990 y la Ley 115 de 1994, las políticas públicas en materia de estímulo y fomento de la ciencia, la tecnología y la innovación, estarán orientadas por los siguientes propósitos:

1. Incrementar la capacidad científica, tecnológica, de innovación y de competitividad del país para dar valor agregado a los productos y servicios de origen nacional y elevar el bienestar de la población en todas sus dimensiones.

2. Incorporar la investigación científica, el desarrollo tecnológico y la innovación a los procesos productivos, para incrementar la productividad y la competitividad que requiere el aparato productivo nacional.

3. Establecer los mecanismos para promover la transformación y modernización del aparato productivo nacional, estimulando la reconversión industrial, basada en la creación de empresas con alto contenido tecnológico y dando prioridad a la oferta nacional de innovación.

4. Integrar esfuerzos de los diversos sectores y actores para impulsar áreas de conocimiento estratégicas para el desarrollo del país.

5. Fortalecer la capacidad del país para actuar de manera integral en el ámbito internacional en aspectos relativos a la ciencia, la tecnología y la innovación.

6. Promover la calidad de la educación formal y no formal, particularmente en la educación media, técnica y superior para estimular la participación y desarrollo de las nuevas generaciones de investigadores, emprendedores, desarrolladores tecnológicos e innovadores.

7. Promover el desarrollo de estrategias regionales para el impulso de la Ciencia, la Tecnología y la Innovación, aprovechando las potencialidades en materia de recursos naturales, lo que reciben por su explotación, el talento humano y la biodiversidad, para alcanzar una mayor equidad entre las regiones del país en competitividad y productividad.

### LEY No .1341 – 30 de Julio del 2009

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - tic-, se crea la agencia nacional de espectro y se dictan otras disposiciones”.

El Congreso de Colombia

DECRETA:

TITULO I

DISPOSICIONES GENERALES

CAPÍTULO I - PRINCIPIOS GENERALES

ARTÍCULO 1.- OBJETO. La presente Ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

ARTÍCULO 2.- PRINCIPIOS ORIENTADORES. La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los derechos humanos inherentes y la inclusión social.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente Ley:

1. Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de / las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación los contenidos y la competitividad.

2. Libre competencia. El Estado propiciará escenarios de libre y leal competencia que incentiven la inversión actual y futura en el sector de las TIC y que permitan la concurrencia al mercado, con observancia del régimen de competencia, bajo precios de mercado y en condiciones de igualdad. Sin perjuicio de lo anterior, el Estado no podrá fijar condiciones distintas ni privilegios a favor de unos competidores en situaciones similares a las de otros y propiciará la sana competencia.

3. Uso eficiente de la infraestructura y de los recursos escasos. El Estado fomentará el despliegue y uso eficiente de la infraestructura para la provisión de redes de telecomunicaciones y los servicios que sobre ellas se puedan prestar, y promoverá el óptimo aprovechamiento de los recursos escasos con el ánimo de generar competencia, calidad y eficiencia, en beneficio de los usuarios, siempre y cuando se remunere dicha infraestructura a costos de oportunidad, sea técnicamente factible, no degrade la calidad de servicio que el propietario de la red viene prestando a sus usuarios y a los terceros, no afecte la prestación de sus propios servicios y se cuente con suficiente infraestructura, teniendo en cuenta la factibilidad técnica y la remuneración a costos eficientes del acceso a dicha infraestructura. Para tal efecto, dentro del ámbito de sus competencias, las entidades de orden nacional y territorial están obligadas a adoptar todas las medidas que sean necesarias para facilitar y garantizar el desarrollo de la infraestructura requerida, estableciendo las garantías y medidas necesarias que contribuyan en la prevención, cuidado y conservación para que no se deteriore el patrimonio público y el interés general.

4. Protección de los derechos de los usuarios. El Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, así como por el cumplimiento de los derechos y deberes derivados del Habeas Data, asociados a la prestación del servicio. Para tal efecto, los proveedores y/u operadores directos deberán· prestar sus servicios a precios de mercado y utilidad razonable, en los niveles de calidad establecidos en los títulos habilitantes o, en su defecto, dentro de los rangos que certifiquen las entidades competentes e idóneas en la materia y con información clara, transparente, necesaria, veraz y anterior, simultánea y de todas maneras oportuna para que los usuarios tomen sus decisiones.

5. Promoción de la Inversión. Todos los proveedores de redes y servicios de telecomunicaciones tendrán igualdad de oportunidades para acceder al uso del espectro y contribuirán al Fondo de Tecnologías de la Información y las Comunicaciones.

6. Neutralidad Tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

7. El Derecho a la comunicación, la información y la educación y los servicios básicos de las TIC: En desarrollo de los artículos 20 y 67 de la Constitución Nacional el Estado propiciará a todo colombiano el derecho al acceso a las tecnologías de la información y las comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos: La libertad de expresión y de difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la educación y el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. Adicionalmente el Estado establecerá programas para que la población de los estratos desarrollará programas para que la población de los estratos menos favorecidos y la población rural tengan acceso y uso a las plataformas de comunicación, en especial de Internet y contenidos informáticos y de educación integral. g

8. Masificación del gobierno en línea. Con el fin de lograr la prestación de servicios eficientes a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones. El Gobierno Nacional fijará los mecanismos y condiciones para garantizar el desarrollo de este principio. Y en la reglamentación correspondiente establecerá los plazos, términos y prescripciones, no solamente para la instalación de las infraestructuras indicadas y necesarias, sino también para mantener actualizadas y con la información completa los medios y los instrumentos tecnológicos.

ARTÍCULO 3.- SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

ARTÍCULO 4.- INTERVENCIÓN DEL ESTADO EN EL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

1. Proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.

2. Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.

3. Promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del gobierno en línea.

4. Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red.

5. Promover y garantizar la libre y leal competencia y evitar el abuso de la posición dominante y las prácticas restrictivas de la competencia.

6. Garantizar el despliegue y el uso eficiente de la infraestructura y la igualdad de oportunidades en el acceso a los recursos escasos, se buscará la expansión, y cobertura para zonas de difícil acceso, en especial beneficiando a poblaciones vulnerables.

7. Garantizar el uso adecuado del espectro radioeléctrico, así como la reorganización del mismo, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.

8. Promover la ampliación de la cobertura del servicio.

9. Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

10. imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.

11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

12. Incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

13. Propender por la construcción, operación y mantenimiento de infraestructuras de las tecnologías de la información y las comunicaciones por la protección del medio ambiente y la salud pública. Parágrafo. El Gobierno Nacional reglamentará lo pertinente al cumplimiento de los anteriores fines, teniendo en cuenta las necesidades de la población y el avance de las tecnologías de la información y las comunicaciones, así como el estado de desarrollo de la Sociedad de la Información en el país, para lo cual, se tendrá en cuenta la participación de todos los actores del proceso, en especial a los usuarios. Se exceptúa de la aplicación de los numerales 4 y 9 de este artículo el servicio de radiodifusión sonora.

Parágrafo. El Gobierno Nacional reglamentará lo pertinente al cumplimiento de los anteriores fines, teniendo en cuenta las necesidades de la población y el avance de las tecnologías de la información y las comunicaciones, así como el estado de desarrollo de la Sociedad de la Información en el país, para lo cual, se tendrá en cuenta la participación de todos los actores del proceso, en especial a los usuarios. Se exceptúa de la aplicación de los numerales 4 y 9 de este artículo el servicio de radiodifusión sonora

ARTÍCULO 6.- DEFINICIÓN DE TIC: Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, vídeo e imágenes.

El Ministerio de Tecnologías de la Información y las Comunicaciones junto con la CRC, deberán expedir el glosario de definiciones acordes con los postulados de la UIT y otros organismos internacionales con los cuales Colombia firmante de protocolos referidos a estas materias.

ARTÍCULO 7.- CRITERIOS DE INTERPRETACIÓN DE LA LEY. Esta Ley se interpretará en la forma que mejor garantice el desarrollo de los principios orientadores establecidos en la misma, con énfasis en la promoción y garantía de libre y leal competencia y la protección de los derechos de los usuarios.

### Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Artículo 3°. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TÍTULO II

PRINCIPIOS RECTORES

Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

TÍTULO III

CATEGORÍAS ESPECIALES DE DATOS

Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Artículo 6°. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Artículo 7°. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

TÍTULO IV

DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

Artículo 8°. Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Artículo 9°. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Artículo 11. Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal, Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley.

Artículo 12. Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;

c) Los derechos que le asisten como Titular;

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

Artículo 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:

a) A los Titulares, sus causahabientes o sus representantes legales;

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;

c) A los terceros autorizados por el Titular o por la ley.

TÍTULO V

PROCEDIMIENTOS

Artículo 14. Consultas. Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Parágrafo. Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

Artículo 15. Reclamos. El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Artículo 16. Requisito de procedibilidad. El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

TÍTULO VI

DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Artículo 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

TÍTULO VII

DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

CAPÍTULO I

De la autoridad de protección de datos

Artículo 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo 1°. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

Parágrafo 2°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

Artículo 20. Recursos para el ejercicio de sus funciones. La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley:

a) Los recursos que le sean destinados en el Presupuesto General de la Nación.

Artículo 21. Funciones. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes;

k) Las demás que le sean asignadas por ley.

CAPÍTULO II

Procedimiento y sanciones

Artículo 22. Trámite. La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Artículo 24. Criterios para graduar las sanciones. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

CAPÍTULO III

Del Registro Nacional de Bases de Datos

Artículo 25. Definición. Reglamentado por el Decreto Nacional 886 de 2014 El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

Parágrafo. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

TÍTULO VIII

TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

Artículo 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Esta prohibición no regirá cuando se trate de:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Parágrafo 2°. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

TÍTULO IX

OTRAS DISPOSICIONES

Artículo 27. Normas Corporativas Vinculantes. El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos, personales y su transferencia a terceros países.

Artículo 28. Régimen de transición. Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

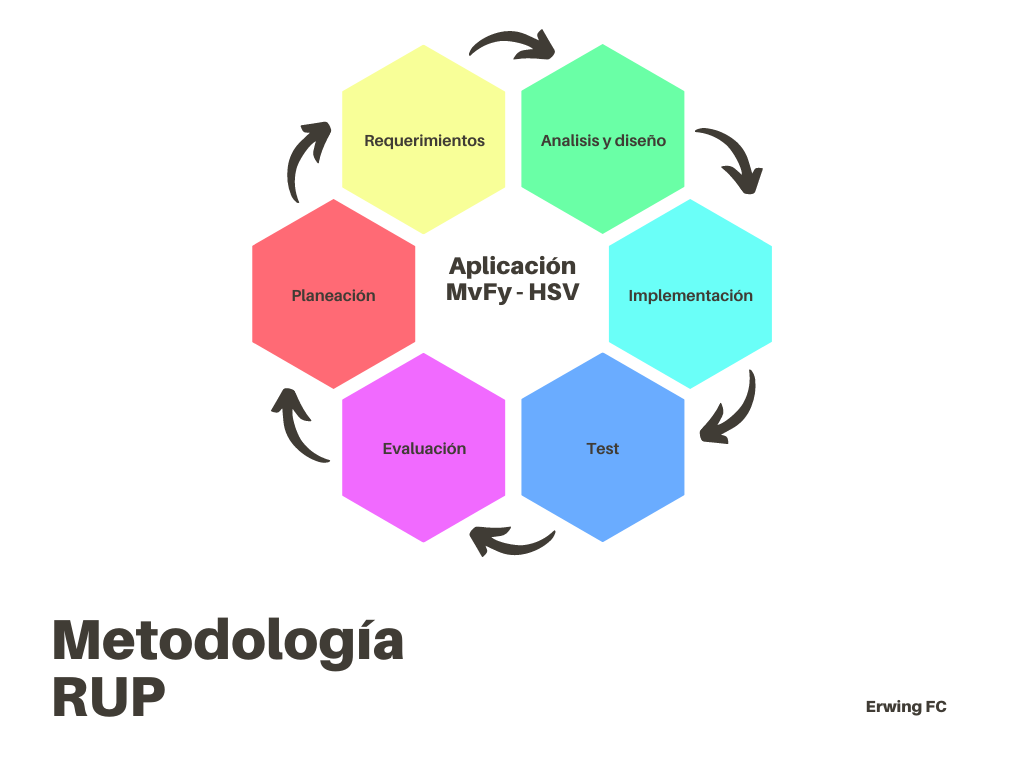
Artículo 29. Derogatorias. La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo 2°.

Artículo 30. Vigencia. La presente ley rige a partir de su promulgación.

# 

# DISEÑO DE LA INVESTIGACION

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



## Fase 1 (Planeación)

En esta fase se realizarán las reuniones necesarias para describir las problemáticas e identificar de forma general la necesidad del proyecto, de forma específica esta fase cuenta con:

* **Esquematización de las reuniones:**  Se realizará un esquema principal de las reuniones que se harán en las semanas posteriores.
* **Estudio de viabilidad:** Se realizará una recopilación de estudios previos en el área, los cuales serán evaluados para determinar posibles casos de uso en un futuro.

## Fase 2 (Requerimientos)

En esta fase se realizará una recolección de requerimientos necesarios que debe cubrir el software, para ello se hará:

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

## Fase 3 (Análisis y Diseño)

Para esta fase se realizará un diseño del funcionamiento principal que debe cubrir la librería, asi como su arquitectura, para ello se realizará:

* **Diseño de la arquitectura:**  se realizará un diseño del seguimiento del uso de la función principal de la librería, asi como los diagramas de caso de uso.
* **Investigación:** para la realización del proyecto se deben tener en cuenta proyectos similares que puedan servir de apoyo en la creación de la libreria.
* **Creación de la documentación:**  se plasmará de forma documental todos los aspectos necesarios que solidifiquen la implementación del proyecto, el presente documento es dicho anexo de ello.

**Fase 4 (Implementación)**

En esta fase se realizará la creación del módulo, para ello se realizará lo siguiente:

* **Desarrollo de la librería:** Se desarrollará el sistema, asi como las pruebas unitarias necesarias para la validación del correcto funcionamiento del mismo.

**Fase 5 (Test)**

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

* **Plan de prueba:** Se realizará un plan de las pruebas a realizar.
* **Pruebas:**  se realizarán las pruebas unitarias y de integración.
* **Solución de problemas:**  si dichas pruebas anteriormente mencionadas resultan de forma negativa, se realizarán las correcciones respectivas y se validarán de nuevo las pruebas.

**Fase 6 (Evaluación)**

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

* **Validación:**  se realizará un recorrido a las funcionalidades del módulo para validar los requerimientos recopilados.

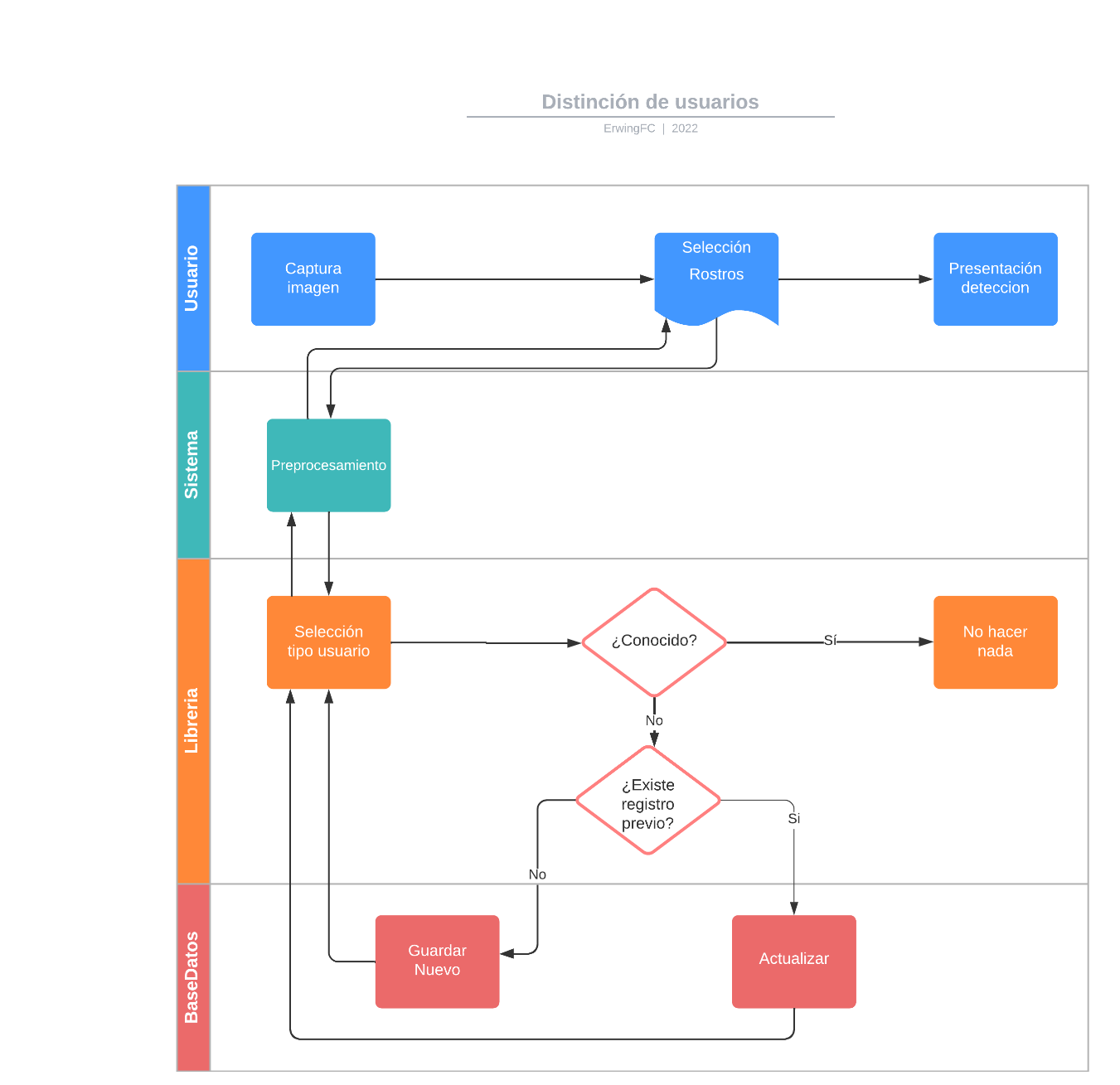
# DESARROLLO DEL TRABAJO DE GRADO

## Análisis y estructura del sistema

### Funcionamiento del sistema

La librería debe proveer de un requerimiento principal que se encarga de todo el proceso denominado **distinción de usuarios** de dicho proceso se derivan las demás funcionalidades.

Figure 5 distinción de usuarios



Fuente: Autor

* **Captura de la imagen**

El sistema espera la recepción de una secuencia de imágenes independientemente de su fuente se esperaría poder captar la informacion por medio del protocolo de transferencia de *websockets[[2]](#footnote-2).*

* **Selección de rostros**

Después de la captura de imagen se procesa la imagen por medio de *OpenCv* [[3]](#footnote-3), para extraer solo la informacion relevante, en este caso los rostros, posteriormente la imagen es segmentada por alguno de los siguientes modelos:

**SSD Mobilenet V1**

Para la detección de rostros, este proyecto implementa un SSD (Single Shot Multibox Detector) basado en MobileNetV1. La red neuronal calculará las ubicaciones de cada rostro en una imagen y devolverá los cuadros delimitadores junto con su probabilidad para cada rostro. Este detector de rostros tiene como objetivo obtener una alta precisión en la detección de cuadros delimitadores de rostros en lugar de un tiempo de inferencia bajo. El tamaño del modelo cuantificado es de unos 5,4 MB (ssd\_mobilenetv1\_model).

**Tiny Face Detector**

El Tiny Face Detector es un detector de rostros en tiempo real de gran rendimiento, que es mucho más rápido, más pequeño y consume menos recursos en comparación con el detector de rostros SSD Mobilenet V1; a cambio, funciona un poco menos bien en la detección de rostros pequeños. Este modelo es extremadamente móvil y compatible con la web, por lo que debería ser su detector de rostros GO-TO en dispositivos móviles y clientes con recursos limitados. El tamaño del modelo cuantificado es de solo 190 KB (tiny\_face\_detector\_model).

El detector de rostros se entrenó en un conjunto de datos personalizado de ~14K imágenes etiquetadas con cuadros delimitadores. Además, el modelo ha sido entrenado para predecir cuadros delimitadores, que cubren por completo los puntos de las características faciales, por lo que, en general, produce mejores resultados en combinación con la detección posterior de puntos de referencia faciales que SSD Mobilenet V1.

Este modelo es básicamente una versión aún más pequeña de Tiny Yolo V2, que reemplaza las circunvoluciones regulares de Yolo con circunvoluciones separables en profundidad. Yolo es completamente convolucional, por lo que puede adaptarse fácilmente a diferentes tamaños de imagen de entrada para compensar la precisión por el rendimiento (tiempo de inferencia).

* **Preprocesamiento**

Este proceso esta relacionado con la implementación, y es un proceso donde la responsabilidad es del desarrollador que lo implemente, es por ello que no se puede prever que proceso se realice, solo se tiene en cuenta como capa intermedia entre el cliente y la librería.

* **Selección tipo usuario**

Para determinar si un usuario es conocido se tendrá el identificador de rostro, este determinaría la autenticidad del usuario y a su vez dicha detección servirá para determinar frecuencia de estancia, para determinar si una de estos usuarios es conocido, se calcula de la siguiente forma:

****

Siendo , la diferencia entre la fecha actual y la fecha inicial de inserción del usuario.



Y el umbral mínimo de diferencia, asi como la frecuencia del

usuario.





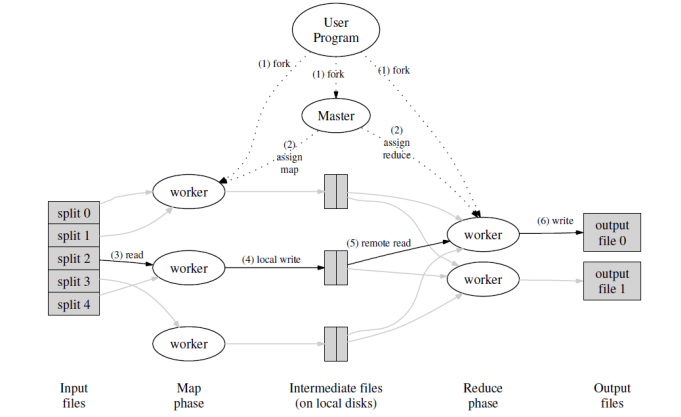
es el valor mínimo de frecuencia, este valor es determinable y se basa la siguiente regla:



### Almacenamiento de los datos

La librería requiere almacenar informacion de forma rápida y flexible es por ello que se opto por el uso de BD, la librería proveería de un driver de conexión, se esperaría poder almacenarla en diferentes tipos de administrador de bases de datos, pero por el momento la opción debido al uso de procesamiento de datos distribuidos vía MapReduce[[4]](#footnote-4) (Strauch)

Figure 6 MapReduce – Execution Overview



Fuente: (Strauch)

## Diseño

### Arquitectura del proyecto

Para el desarrollo de la librería se implementó una de las *arquitecturas limpias[[5]](#footnote-5)*, denominada como “Onion Architecture”, manteniendo asi una alta escalabilidad no solo en las funcionalidades, si no, tambien una alta mantenibilidad ya que se espera la mejora y adición de funcionalidades en un futuro.

Figure 7 Clean Architecture



Fuente: (Martin, 2012)

* **Entidades**

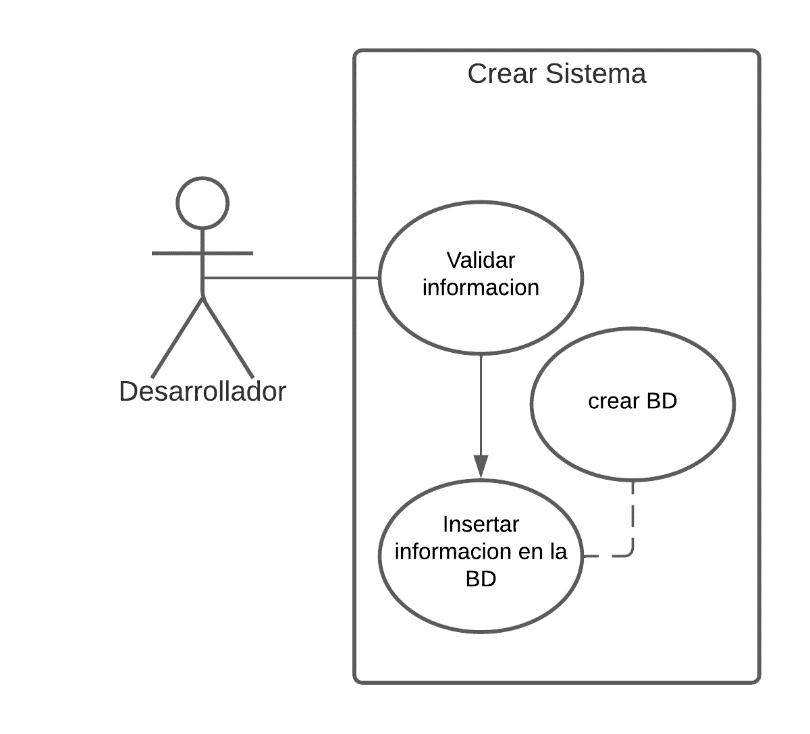
Para la librería posee las siguientes entidades:

|  |  |
| --- | --- |
| Users | |
| propiedad | **descripción** |
| \_id | Identificador único |
| systemId | Identificador del sistema (Entity.systems.\_id) |
| author | nombre |
| detection | Detección del rostro |
| properties | Propiedades del usuario |
| initDate | Fecha inicial de detección |
| lastDate | Ultima fecha de detección |
| knowledge | ¿conocido? |
| frequency | Frecuencia de detección del usuario |

|  |  |
| --- | --- |
| Systems | |
| propiedad | **descripción** |
| \_id | Identificador único |
| type\_service | Tipo de servicio, se espera que el uso pueda darse en dos ambientes: local y remoto. |
| max\_descriptor\_distance | Umbral máxima del descriptor |
| min\_date\_knowledge | Margen mínimo para determinar si un usuario es conocido |
| min\_frequency | Frecuencia minima entre detecciones |
| features | Características adicionales: detección de edad, genero u expresiones |
| type\_system | Tipo de sistema: optimizado o preciso |
| title | Titulo opcional del sistema |

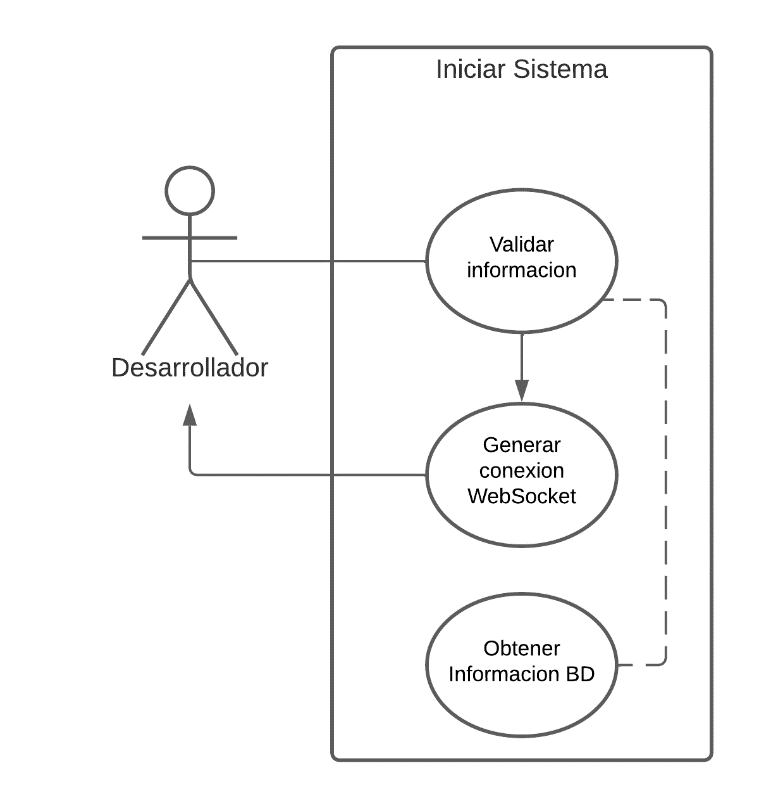
* **Casos de uso**

Figure 8 crear sistema



Fuente: Autor

Figure 9 Iniciar sistema



Fuente: Autor

* **Interfaces Externas**

La librería posee diferentes dependencias externas entre ellas se encuentran las siguientes:

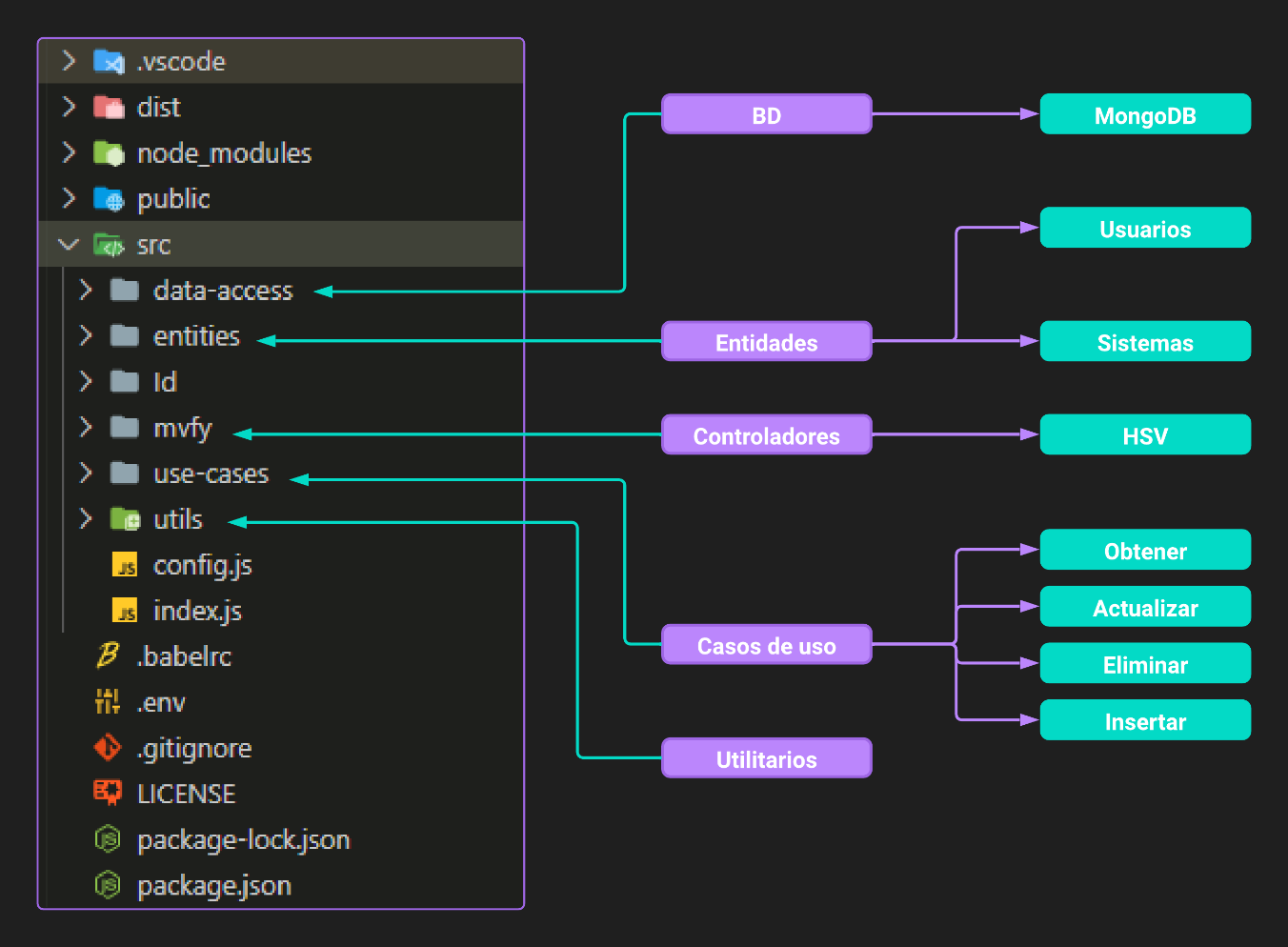
1. Base de datos: MongoDB
2. Framework: Nodejs
3. Compilador: babel
4. Procesador de imágenes: OpenCV

## Desarrollo

### Estructura de carpetas

Implementando la arquitectura mencionada con anterioridad se segmento el proyecto de la siguiente forma:

Figure 10 estructura de carpetas



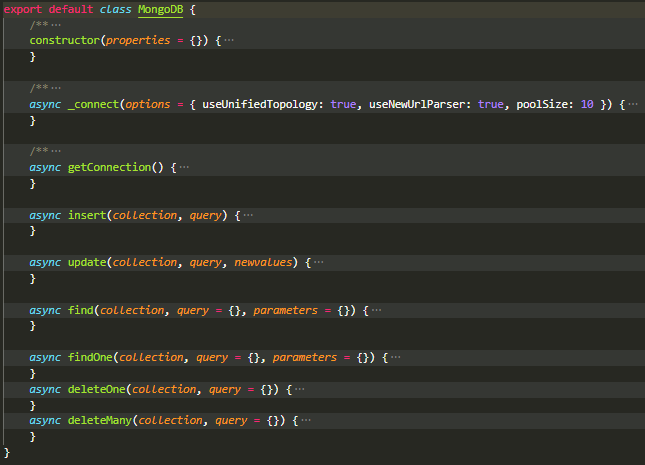
Fuente: Autor

### Acceso de datos

Para el acceso de datos se uso el driver provisto por MongoDB, para ello se proporcionó de una clase que se encarga de lo siguiente:

* Class MongoDB: proporciona el manejo de la base de datos

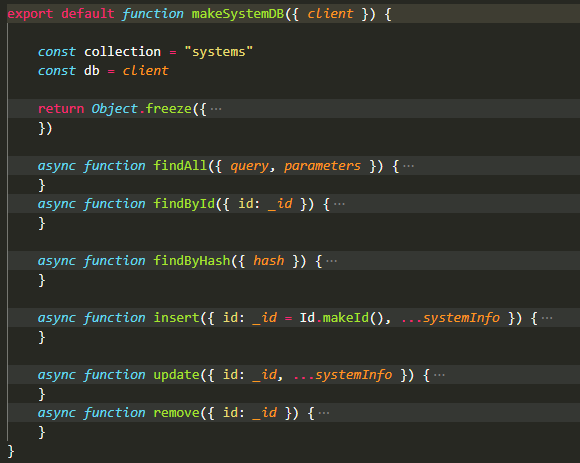
Figure 11 Class MongoDB.



Fuente: Autor

* Function makeSystemDB: extiende las funcionalidades de mongodb, para el manejo de informacion de los usuarios.

Figure 12 MakeSystemDB



Fuente: Autor

* Function makeUserDB: extiende las funcionalidades de mongodb, para el manejo de informacion del sistema.

Figure 13 makeUserDB

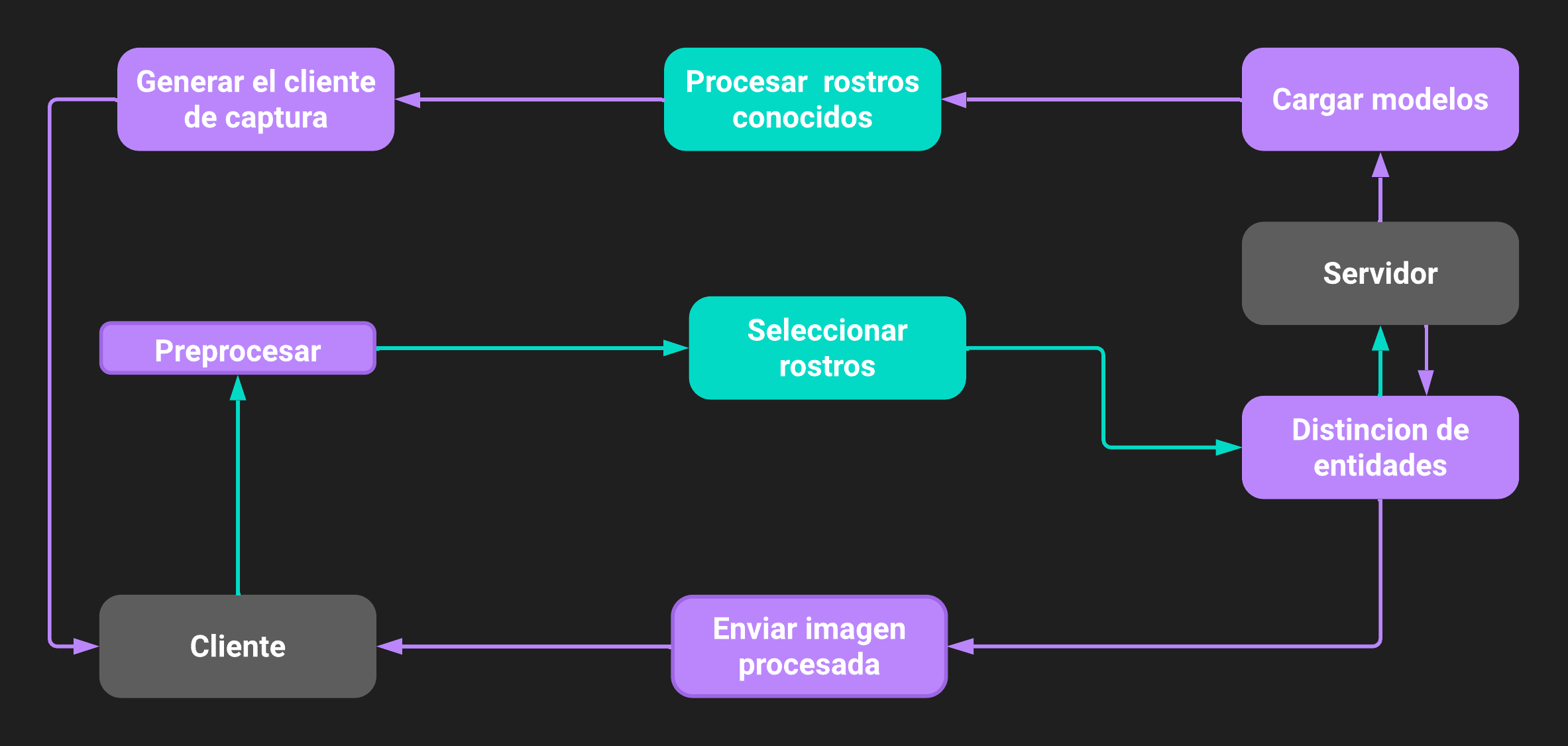


Fuente: Autor

### Controladores

El principal controlador y único es *MvfyHsv,* el cual se encarga de manejar la informacion proporcionada por los *use-cases,* dentro de las multiples funcionalidades se sigue el siguiente proceso principal:

Figure 14 proceso principal



Fuente: Autor

* **Cargar modelos**

Al iniciar el sistema se cargan los modelos usados en el proceso de selección de rostros, dichos modelos se diferencian en el [funcionamiento del sistema](#_Funcionamiento_del_sistema).

* **Procesar rostros conocidos**

Después de cargar los modelos se obtiene la informacion de la BD de los usuarios pertenecientes al sistema, se procesan los descriptores de los rostros para obtener un clasificador capaz de distinguir a los usuarios conocidos de desconocidos.

* **Generar el cliente de captura**

Si el desarrollador no provee de una conexión de cliente, se genera un archivo html en el navegador que se conecta con el servidor mostrando la informacion capturada por la cámara.

* **Preprocesar**

Se procesa la imagen capturada para mantener las dimensiones, asi como el formato esperado por el modelo de selección de rostros.

* **Seleccionar Rostros y distinción de entidades**

Este modelo fue detallado en [funcionamiento del sistema](#_Funcionamiento_del_sistema).

Para proporcionar una implementación sencilla del módulo se desarrolló una clase que sería 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.

# RESULTADOS

Pendiente.

# 

# CONCLUSIONES

Pendiente

# 

# 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, añadir autenticación y middlewares para aumentar la seguridad en la transferencia de información.
2. Se recomienda añadir funcionalidades para mejorar la interoperabilidad entre la librería y sistemas de seguridad complejos que no se hayan tenido en cuenta.
3. Se sugiere que al ser implementado, se proporcione una alerta al cliente indicando que dicho sistema es semiautomatizado y requiere de la intervención humana.
4. La librería se encuentra en una fase beta anterior al lanzamiento del producto, por lo que se espera sus usos estén por fuera de ambientes de producción.
5. La librería tiene gran margen de mejora, debido a limitaciones por parte del autor, por lo que es posible refactorizar u actualizar funciones con el propósito de mejora.

# 

# 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

## Apéndice 1

# ANEXOS

**Instructivo General[[6]](#footnote-6)**

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**

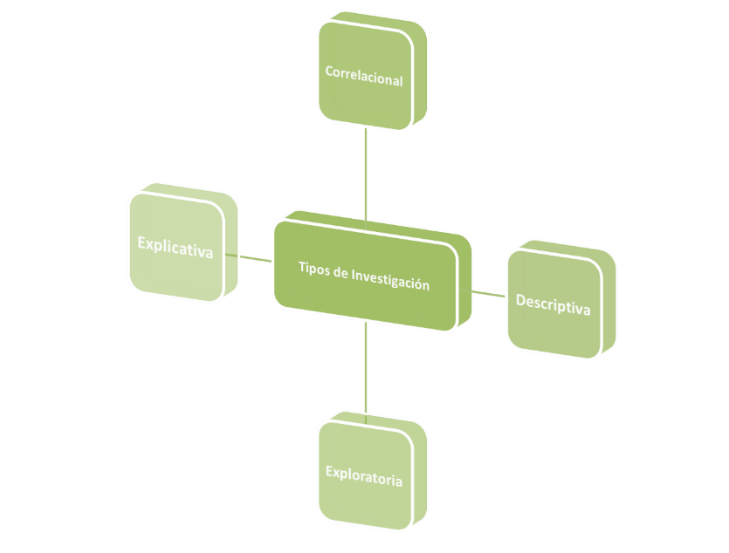
Esta sección del documento es de orientación para la elaboración del documento, **debe eliminarla** cuando genere la versión final. De igual manera, **debe eliminar** todas las instrucciones que contiene esta plantilla, que por lo general las encontrará como texto en color gris.

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. Rand es una “organización de investigación que desarrolla soluciones a los desafíos de las políticas públicas para ayudar a que las comunidades de todo el mundo sean más seguras, saludables y prósperas” - Rand [↑](#footnote-ref-1)
2. Websocket es una tecnología que proporciona un canal de comunicación bidireccional y full-duplex sobre un único socket TCP. [↑](#footnote-ref-2)
3. OpenCv es una biblioteca libre de visión artificial originalmente desarrollada por Intel. [↑](#footnote-ref-3)
4. Mapreduce es un paradigma de programación que permite una escalabilidad masiva en cientos o miles de servidores en un clúster de Hadoop. [↑](#footnote-ref-4)
5. Arquitectura limpia es Independiente de los frameworks, Testable, Independiente de la UI, Independiente de la base de datos e Independiente de cualquier entidad externa. [↑](#footnote-ref-5)
6. 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-6)