

HSV - Modulo de seguridad de reconocimiento facial

Erwing Forero Castro

Systems Engineer and data scientists

2020

Contenido

[HSV - Modulo de seguridad de reconocimiento facial 1](file:///D:\Proyectos\Face%20Recognition\Documents\Tarea2_Erwing_Forero.docx#_Toc53775557)

[**1.** **HISTORIA** 3](#_Toc53775558)

[**2.** **RESUMEN** 4](#_Toc53775559)

[**Bibliografia** 10](#_Toc53775560)

[ Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online. ACM Comput. Surv. 50, 3, Article 44 (October 2017), 41 pages. 10](#_Toc53775561)

[ MORA (2019), Hector. Manual del vigilante de seguridad. Editirial Club Univeritario. Madrid. 10](#_Toc53775562)

[ 10](#_Toc53775563)

1. **HISTORIA**

Partiendo de la necesidad de superar cada vez más nuestras limitaciones tecnológicas, las cuales, nos han llevado desde que suponemos aparecimos por primera vez los Homo sapiens (del latín, homo ‘hombre’ y sapiens ‘sabio’) a realizar tareas más complejas que puedan suplir una necesidad muy demandada, tal es el caso de la famosa invención de la rueda, llevándonos hasta la máquina de vapor en 1890, de ahí a la energía nuclear o atómica en 1942, el ordenador en 1936, la invención de los cohetes y la conquista espacial, saltos demasiado grandes verdad, pues hoy queremos realizar un salto lo suficientemente alto como para crearnos a nosotros mismos o algo similar a ello.

La inteligencia artificial es la puerta a esa gran idea, que hace unos años parecía imposible, pues en su comienzo de IA tenemos al gran Alan Turing quien se le atribuye la invención de la “Máquina de Turing” cuyo objetivo era romper o desencriptar los códigos de la maquina “Enigma” maquinas usadas por los alemanes en la segunda mundial usados para la comunicación interna, ayudando así de forma muy sutil a la terminación de la segunda guerra mundial, salvando miles de vidas; también se le atribuye uno de los test mas famosos, denominado el test de Turing, el cual, consiste en preguntar a una maquina (sin saber que lo es) preguntas aleatorias si la persona quien hizo el test no llega a darse cuenta de que está preguntándole a una maquina se podría determinar que la maquina es tan inteligente como un humano.

En 1952 Arthur Samuel escribe el primer programa de ordenador capaz de aprender, el algoritmo era un programa que jugaba a las damas y que mejoraba su juego partida tras partida. En 1956 Martin Minsky y John McCarthy, con la ayuda de Claude Shannon y Nathan Rochester, organizan la conferencia de Darthmouth de 1956, considerada como el evento donde nace el campo de la Inteligencia Artificial. Durante la conferencia, Minsky convence a los asistentes para acuñar el término “Artificial Intelligence” como nombre del nuevo campo.

En 1958 Frank Rosenblatt diseña el Perceptrón, la primera red neuronal artificial. En 1981 — Gerald Dejong introduce el concepto “Explanation Based Learning” (EBL), donde un computador analiza datos de entrenamiento y crea reglas generales que le permiten descartar los datos menos importantes. En 2011 — El ordenador Watson de IBM vence a sus competidores humanos en el concurso Jeopardy que consiste en contestar preguntas formuladas en lenguaje natural. En 2016 – Google DeepMind vence en el juego Go (considerado uno de los juegos de mesa más complicados) al jugador profesional Lee Sedol por 5 partidas a 1. Jugadores expertos de Go afirman que el algoritmo fue capaz de realizar movimientos “creativos” que no se habían visto hasta el momento [victor gonzales (2019)](https://empresas.blogthinkbig.com/una-breve-historia-del-machine-learning/).

1. **RESUMEN**

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

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

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

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

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

1. **INTRODUCCIÓN**

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

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

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

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

1. **DESCRIPCIÓN DE LA PROBLEMÁTICA**

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

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

* 1. **Herramienta, no sistema**

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

* 1. **Politica de privacidad**

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

* 1. **¿Son los desconocidos los unicos problematicos?**

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

1. **JUSTIFICACIÓN**

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

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

1. **OBJETIVOS**
   1. **Objetivo principal**

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

* 1. **Objetivos especificos**
* Investigar implementaciones robustas de sistemas similares de reconocimiento facial y esquemas de modelos altamamente eficientes.
* Planear y diseñar la estructura de funciones que solventara en un posible sistema.
* Desarrollar el modulo de seguridad de reconocimiento facial.
* Realizar las pruebas unitarias.
* Publicar el ensayo investigativo sobre el modulo.

1. **ESTADO DEL ARTE**

**7.1. MediaPipe Iris: seguimiento del iris en tiempo real (Google 2020)**

Este modelo, hace parte de una 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, MediaPipe, 2020)

**7.2. MediaPipe face detector (Google 2020**

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. (Google, 2020).

**7.3 Elastic Bunch Graph Matching (EBGM)**

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.

1. **ANTECEDENTES**

**8.1. MEDICIONES MANUALES POR BLEDSOE (1960)**

Muchos dirían que el padre del reconocimiento facial fue Woodrow Wilson Bledsoe. Trabajando en la década de 1960, Bledsoe desarrolló un sistema que podía clasificar fotos de rostros a mano utilizando lo que se conoce como una tableta RAND, un dispositivo que las personas podían usar para ingresar coordenadas horizontales y verticales en una cuadrícula utilizando un lápiz óptico que emitía pulsos electromagnéticos. El sistema podría usarse para registrar manualmente las ubicaciones de coordenadas de varias características faciales, incluidos los ojos, la nariz, la línea del cabello y la boca.

Estas métricas podrían insertarse en una base de datos. Luego, cuando el sistema recibió una nueva fotografía de un individuo, fue capaz de recuperar la imagen de la base de datos que más se parecía a esa persona. En ese momento, el reconocimiento facial por desgracia estaba limitado severamente por la tecnología de la era y el poder de procesamiento de la computadora. Sin embargo, fue un primer paso importante para probar que el reconocimiento facial era una biometría viable.

**8.2. IMAYOR PRECISIÓN CON 21 MARCADORES FACIALES (1970)**

En la década de 1970, Goldstein, Harmon y Lesk fueron capaces de agregar una mayor precisión a un sistema de reconocimiento facial manual. Utilizaron 21 marcadores subjetivos específicos, incluidos el grosor del labio y el color del cabello, para identificar caras automáticamente. Al igual que con el sistema de Bledsoe, la biometría real tuvo que ser aún computada manualmente.

**8.3. EIGENFACES (FINALES DE 1980 – PRINCIPIOS DE 1990)**

En 1988, Sirovich y Kirby comenzaron a aplicar el álgebra lineal al problema del reconocimiento facial. Lo que se conoció como el enfoque Eigenface comenzó como una búsqueda de una representación de baja dimensión de las imágenes faciales. Sirovich y Kriby pudieron demostrar que el análisis de las características de una colección de imágenes faciales podría formar un conjunto de características básicas. También pudieron demostrar que se necesitaban menos de cien valores para codificar con precisión una imagen de cara normalizada.

En 1991, Turk y Pentland ampliaron el enfoque Eigenface descubriendo cómo detectar rostros dentro de las imágenes. Esto condujo a las primeras instancias de reconocimiento facial automático. Su enfoque se vio limitado por factores tecnológicos y ambientales, pero fue un gran avance en la demostración de la viabilidad del reconocimiento facial automático.

**8.4. PROGRAMA FERET (1993-2000)**

La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) y el Instituto Nacional de Estándares y Tecnología lanzaron el programa de Tecnología de Reconocimiento Facial (FERET) a partir de la década de 1990 con el fin de fomentar el mercado de reconocimiento facial comercial. El proyecto involucró la creación de una base de datos de imágenes faciales. La base de datos se actualizó en 2003 para incluir versiones en color de alta resolución de 24 bits. Incluido en el conjunto de prueba fueron 2.413 imágenes faciales todavía que representan 856 personas. La esperanza era que una gran base de datos de imágenes de prueba para el reconocimiento facial podría inspirar la innovación, que podría dar como resultado una tecnología de reconocimiento facial más poderosa.

**8.5. SUPER BOWL XXXV (2002)**

En el Super Bowl de 2002, los funcionarios encargados de hacer cumplir la ley utilizaron el reconocimiento facial en una prueba importante de la tecnología. Si bien los funcionarios informaron que se detectaron varios “delincuentes menores”, en general, la prueba fue vista como un fracaso. Los falsos positivos y la reacción de los críticos demostraron que el reconocimiento facial no estaba del todo preparado para el horario de máxima audiencia. Una de las grandes limitaciones tecnológicas de la época era que el reconocimiento facial aún no funcionaba bien en grandes multitudes, una funcionalidad que es esencial para usar el reconocimiento facial para la seguridad de eventos.

**8.6. PRUEBAS DE PROVEEDORES DE RECONOCIMIENTO FACIAL (2000)**

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) comenzó las Pruebas de reconocimiento facial (FRVT) a principios de la década de 2000. Partiendo de FERET, los FRVT se diseñaron para proporcionar evaluaciones gubernamentales independientes de los sistemas de reconocimiento facial que estaban disponibles comercialmente, así como también tecnologías de prototipo. Estas evaluaciones se diseñaron para proporcionar a las agencias encargadas de hacer cumplir la ley y al gobierno de EE. UU. La información necesaria para determinar las mejores formas de implementar la tecnología de reconocimiento facial.

**8.7. BASE DE DATOS FORENSES DE APLICACIÓN DE LA LEY (2009)**

En 2009, la Oficina del Alguacil del Condado de Pinellas creó una base de datos forense que permitía a los oficiales acceder a los archivos de fotos del Departamento de Seguridad Vial y Vehículos Motorizados (DHSMV) del estado. Para 2011, unos 170 diputados habían sido equipados con cámaras que les permitían tomar fotografías de sospechosos que podrían cotejarse con la base de datos. Esto resultó en más arrestos e investigaciones criminales de lo que hubiera sido posible de otro modo.

**8.9. MEDIOS SOCIALES (2010-PRESENTE)**

A partir de 2010, Facebook comenzó a implementar la funcionalidad de reconocimiento facial que ayudó a identificar a las personas cuyas caras pueden aparecer en las fotos que los usuarios de Facebook actualizan a diario. Si bien la función fue instantáneamente controvertida con los medios de comunicación, lo que generó una gran cantidad de artículos relacionados con la privacidad, a los usuarios de Facebook en general no pareció importarles. Al no tener un impacto negativo aparente en el uso o la popularidad del sitio web, más de 350 millones de fotos se cargan y etiquetan mediante el reconocimiento facial cada día.

**8.10. PRIMERA INSTALACIÓN PRINCIPAL DEL RECONOCIMIENTO FACIAL EN UN AEROPUERTO (2011)**

En 2011, el gobierno de Panamá se asoció con el entonces gobierno de los EE. UU. La secretaria de Seguridad Nacional, Janet Napolitano, autorizó un programa piloto de la plataforma de reconocimiento facial de FaceFirst para reducir la actividad ilícita en el aeropuerto Tocumen de Panamá (conocido como un centro para el contrabando de drogas y el crimen organizado).

Poco después de la implementación, el sistema resultó en la aprehensión de múltiples sospechosos de Interpol. Satisfecho con el éxito del despliegue inicial, FaceFirst se expandió a la terminal norte de la instalación. La implementación de FaceFirst en Tocumen sigue siendo la instalación biométrica más grande en un aeropuerto hasta la fecha.

**8.11. LAS AGENCIAS DE APLICACIÓN DE LA LEY ADOPTAN EL RECONOCIMIENTO DE LA CARA MÓVIL (2014)**

A partir de 2014, el Sistema Automatizado de Información de Justicia Regional (ARJIS), comenzó a suministrar a las agencias asociadas la plataforma móvil FaceFirst que admite reconocimiento facial para la aplicación de la ley. ARJIS, una compleja red de empresas de justicia penal que promueve la información y el intercambio de datos entre las agencias policiales locales, estatales y federales, quería resolver un problema crítico: la identificación instantánea para las personas que no tenían identificación o no deseaban ser identificadas. Algunas de las agencias que comenzaron a utilizar el reconocimiento facial móvil para identificar sospechosos en el campo incluyen a la policía de San Diego, DOJ, FBI, DEA, CBP y Marshalls de los EE. UU.

1. **MARCO REFERENCIAL**

**9.1. MARCO TEORICO**

**9.1.1. Deep learning, Machine learning e inteligencia artificial**

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

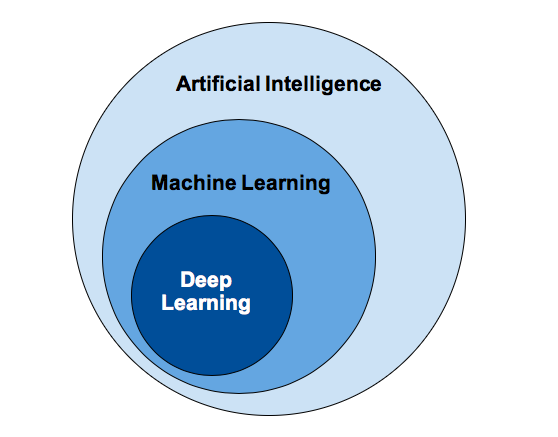


Figure 1 Inteligencia Artificial, Machine Learning y Deep Learning

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

**9.1.2. 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.

**9.1.3. 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.

**9.1.4. 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.

**9.1.5. Redes Neuronales Artificiales (RNA)**

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

animales.

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

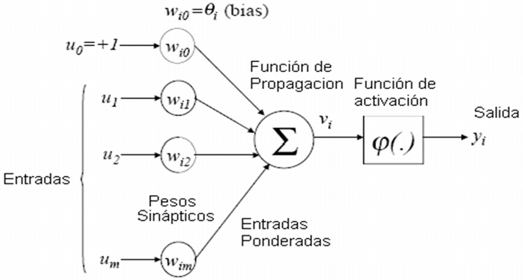


Figure 2Neurona artificial

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

**Sigmoid: 𝑓(𝑥) = 2/1+𝑒−2𝑥 – 1**

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

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

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

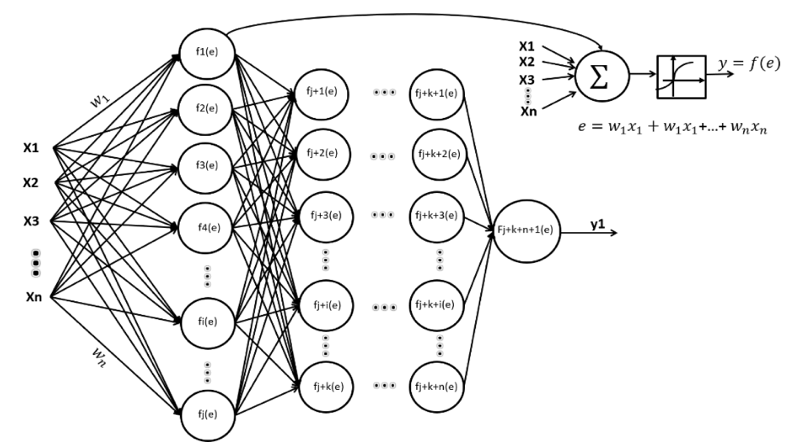


Figure 3Red neuronal artificial

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

**9.1.6. 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).

**9.1.7. 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.

**9.1.8. 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

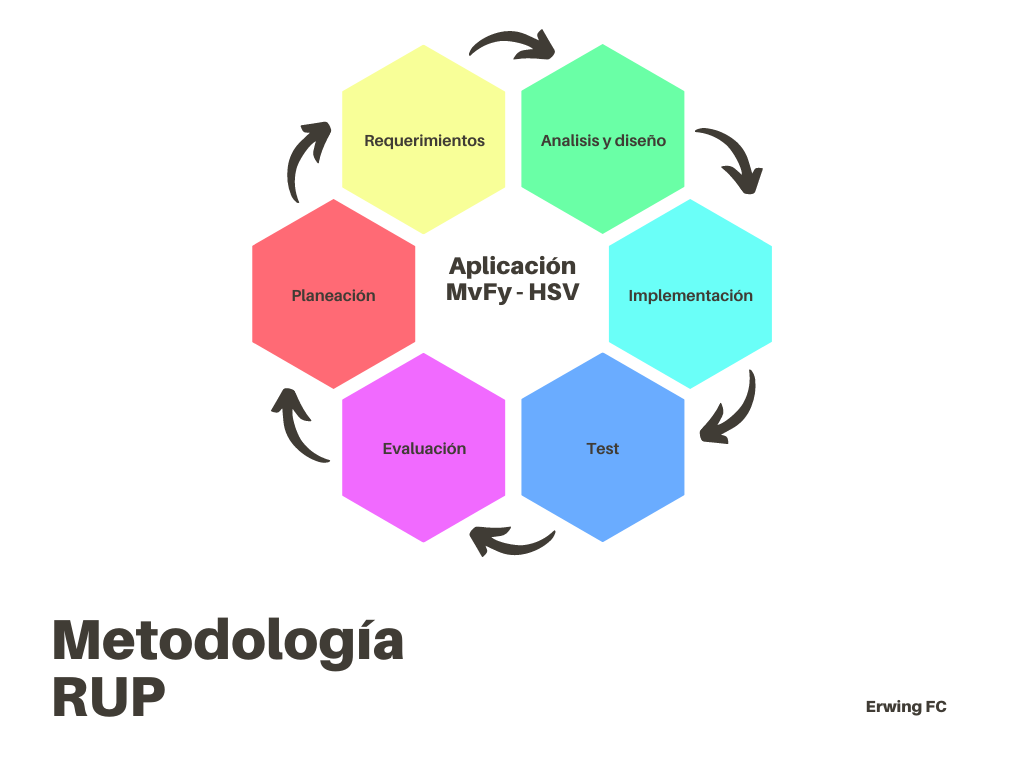
En estas redes, se cuenta con patrones conocidos y bien categorizados, con el fin de clasificar de forma directa.

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.

1. **METODOLOGIA**

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



**Fase 1 ( Planeación )**

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

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

**Fase 2 ( Requerimientos)**

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

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

**Fase 3 ( Analisis y Diseño )**

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

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

**Fase 4 ( Implementacion )**

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

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

**Fase 5 ( Test )**

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

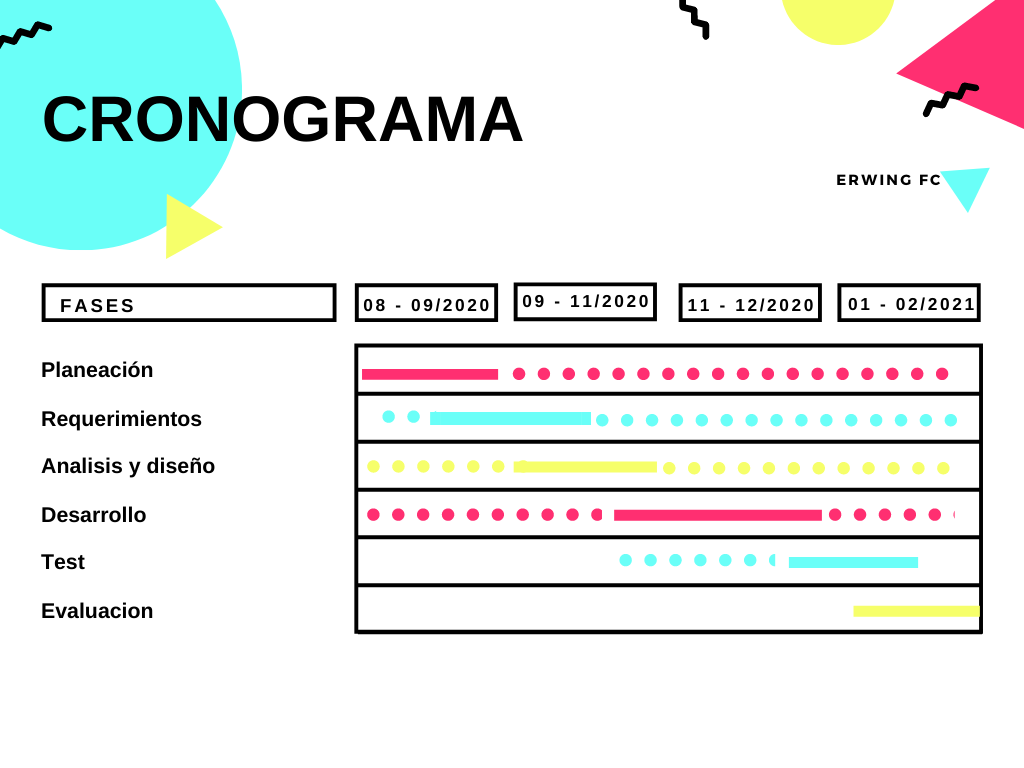
* **Plan de prueba:** Se realizara un plan de las pruebas a realizar.
* **Pruebas:**  se realizaran las pruebas unitarias y de integracion.
* **Solucion de problemas:**  si dichas pruebas anteriormente mencionadas resultan de forma negativa, se realizaran las correcciones respectivas y se validaran de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

**Fase 6 ( Evaluacion )**

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

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

1. **Cronograma**

****