ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Sistema de prueba de vida para login biométrico usando modelos de machine learning

Cáceres Erraez Cristóbal Alejandro

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

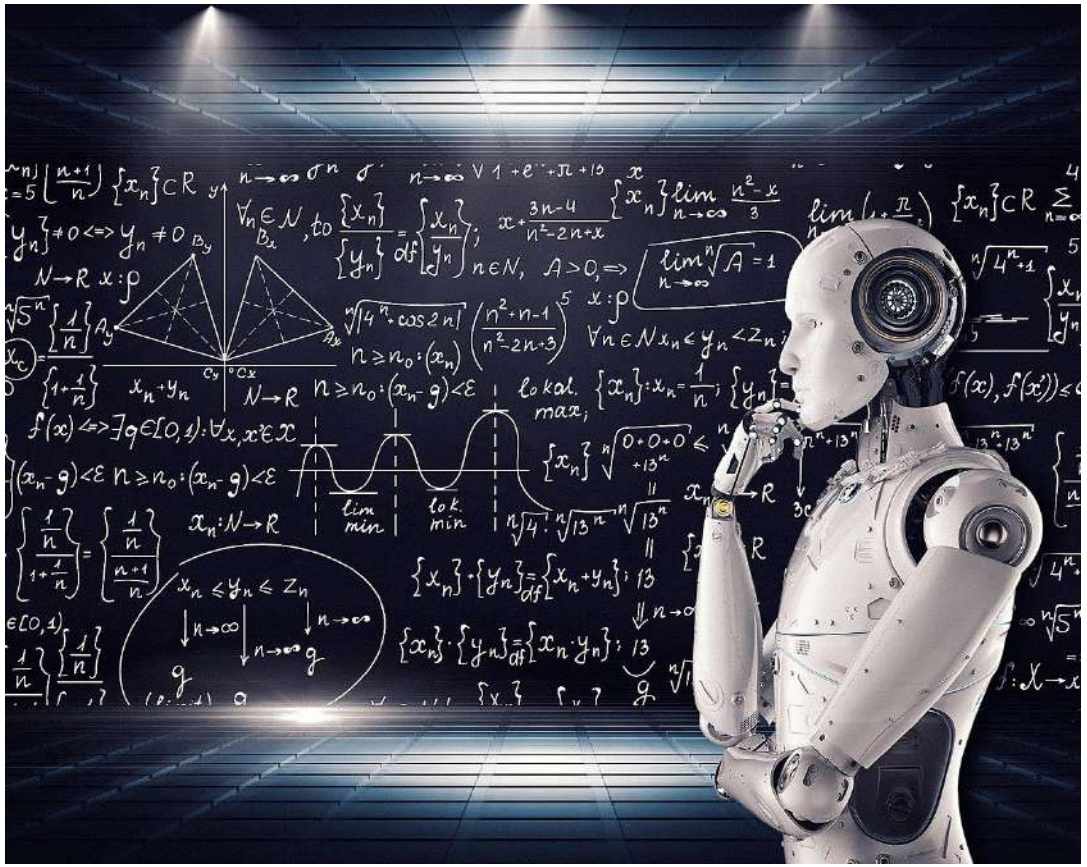
Msc. Delgado Rodríguez, Ramiro Nanac

24 de agosto del 2022

AGENDA

1. Introducción, Objetivos y Alcance
2. Descripción del proyecto
3. Desarrollo del Sistema
4. Análisis de resultados
5. Conclusiones y Recomendaciones

INTRODUCCIÓN



Determinar si una persona esta viva o no, para un humano puede ser relativamente fácil… pero para un programa?

Es aquí donde el uso de modelos de inteligencia artificial nos facilitan el desarrollo de diversas soluciones, en este caso una prueba de vida.

Se va a tocar superficialmente el gran campo de la Inteligencia Artificial para poner en contexto la potencia de las herramientas que se encuentran en nuestras manos

OBJETIVOS

General:

Diseñar un sistema de prueba de vida para login biométrico en web usando modelos de machine learning.

Específicos:

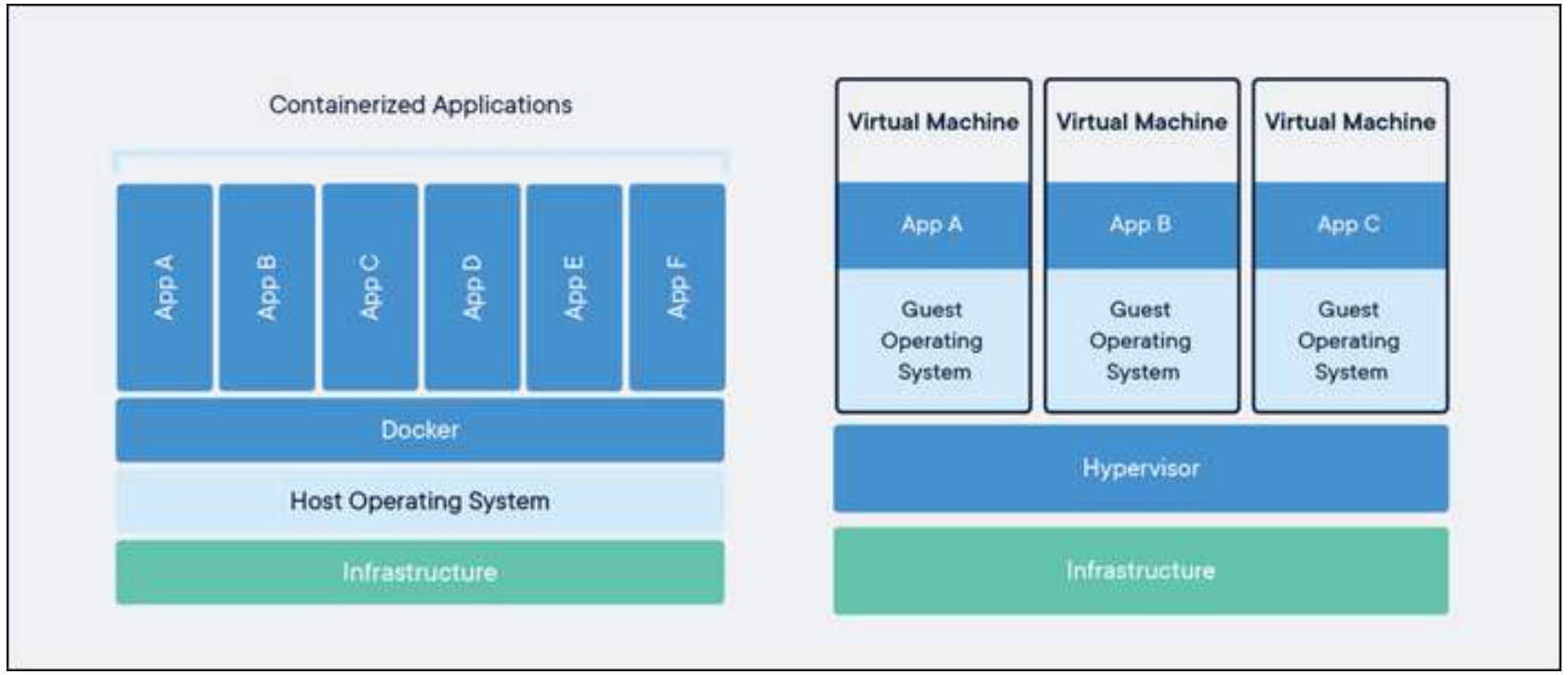
- Investigar modelos de machine learning que permitan el reconocimiento facial.
- Investigar sobre el uso del paradigma de servicios web para la codificación del sistema web
- Diseñar una solución que permita la integración de los servicios de prueba de vida para el proveedor de identidades y accesos keycloak.
- Realizar pruebas y evaluar resultados.

ALCANCE

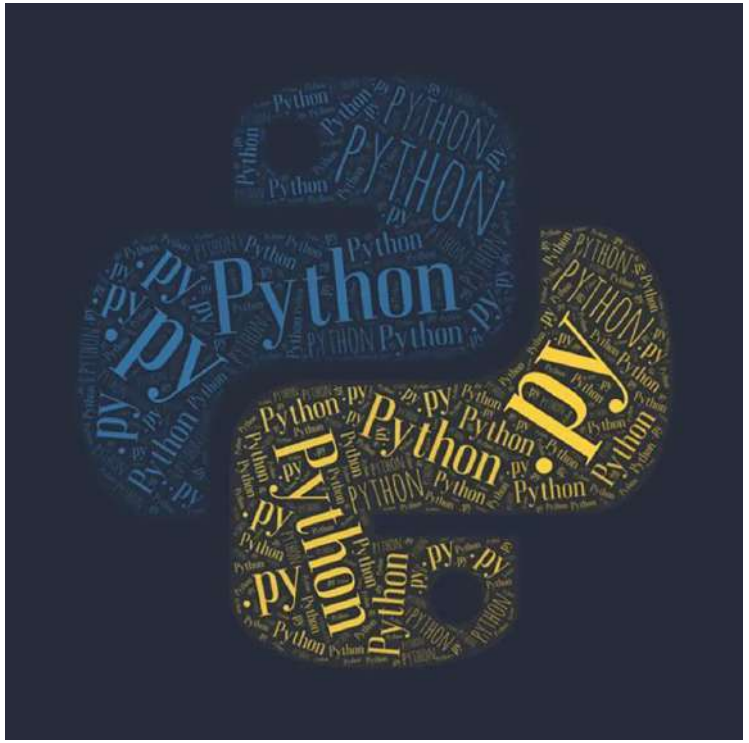
Se planteó como alcance original el desarrollo de una API que contenga la lógica del sistema de prueba de vida para login biométrico y una página web para poder realizar las pruebas del funcionamiento correcto de la misma.

Adicional al alcance original se generó la integración en el proveedor de identidades keycloak para generar un flujo funcional de webs segurizadas.

DOCKER


Containerized Applications
App A
App B
App C
App D
App E
App F
Docker
Host Operating System
Infrastructure
Virtual Machine
Virtual Machine
Virtual Machine
App A
App B
App C
Guest Operating System
Guest Operating System
Guest Operating System
Hypervisor
Infrastructure

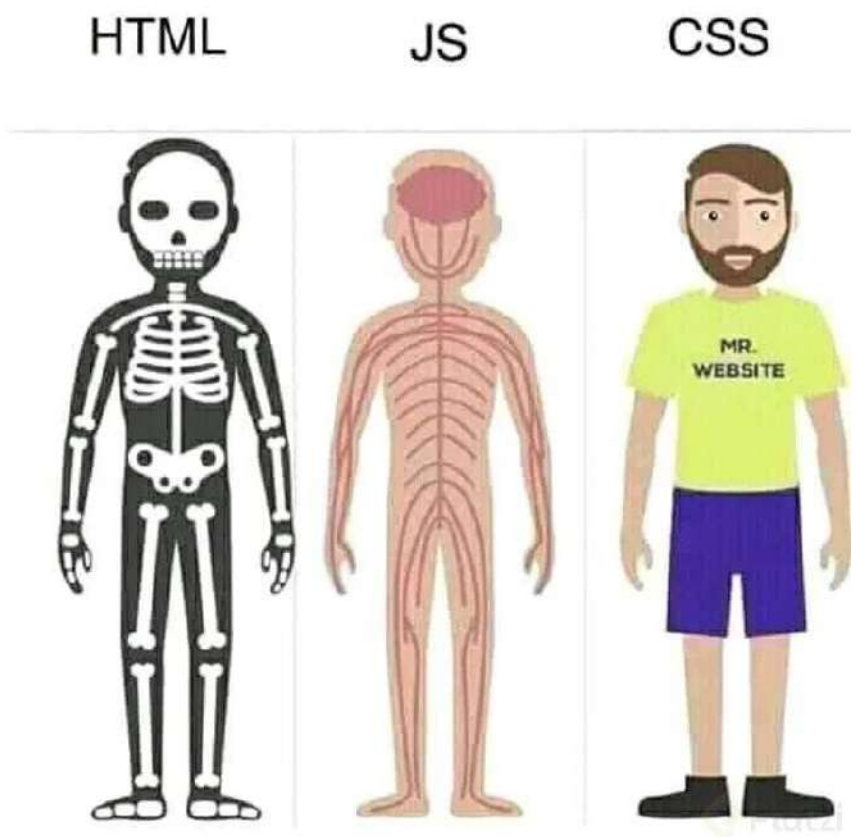
PYTHON



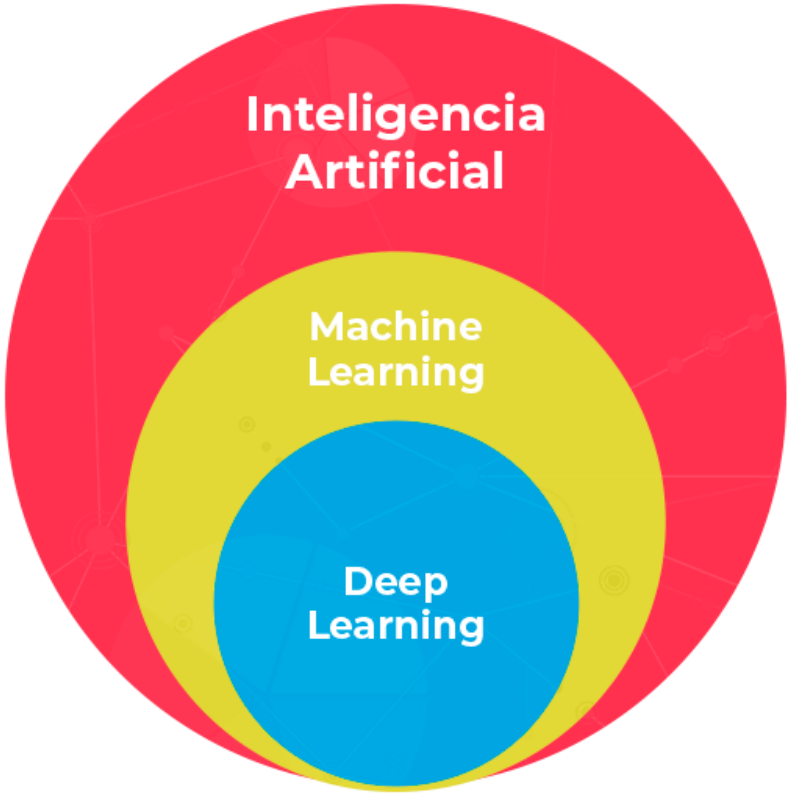
“Python es un lenguaje de programación que permite trabajar rápidamente e integrar sistemas de manera más efectiva.” (Python, 2021)

En el campo de la Inteligencia Artificial es muy común el uso de este lenguaje para el desarrollo de soluciones, por la facilidad y gran cantidad de información que se puede encontrar en internet es el lenguaje que se utilizó en el desarrollo del API de este proyecto

HTML, CSS, JS



INTELIGENCIA ARTIFICIAL

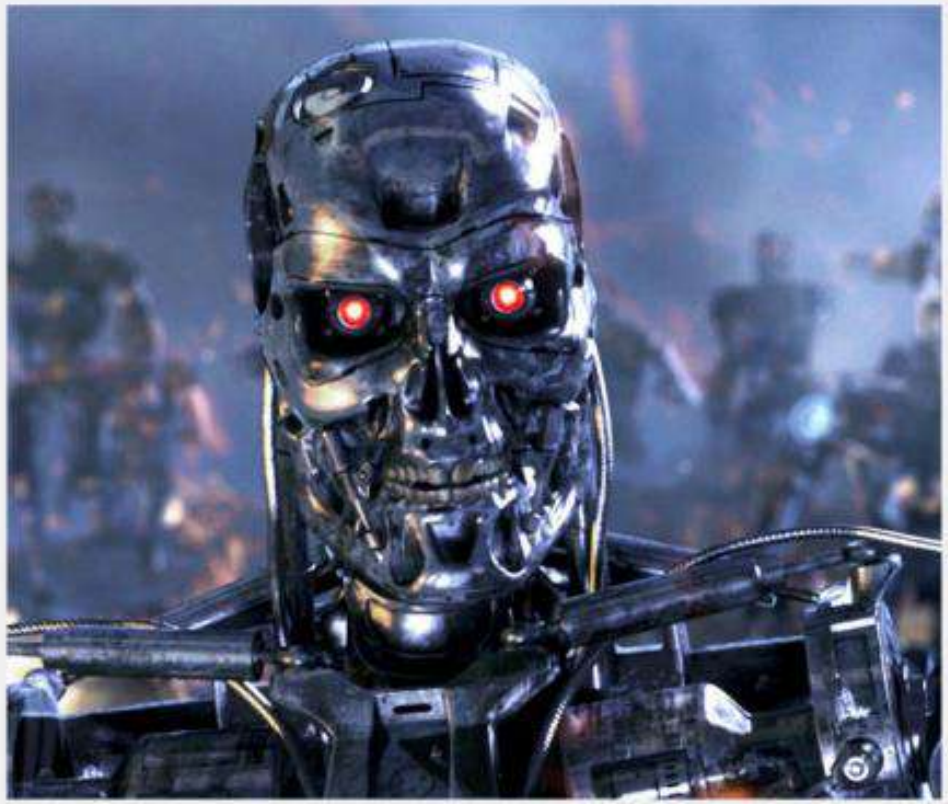


IA: Combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.

Machine Learning: Rama de la Inteligencia artificial (IA) que estudia como dotar a las máquinas de capacidad de aprendizaje

Deep Learning: algoritmo automático jerárquico que emula el aprendizaje humano con el fin de obtener ciertos conocimientos.

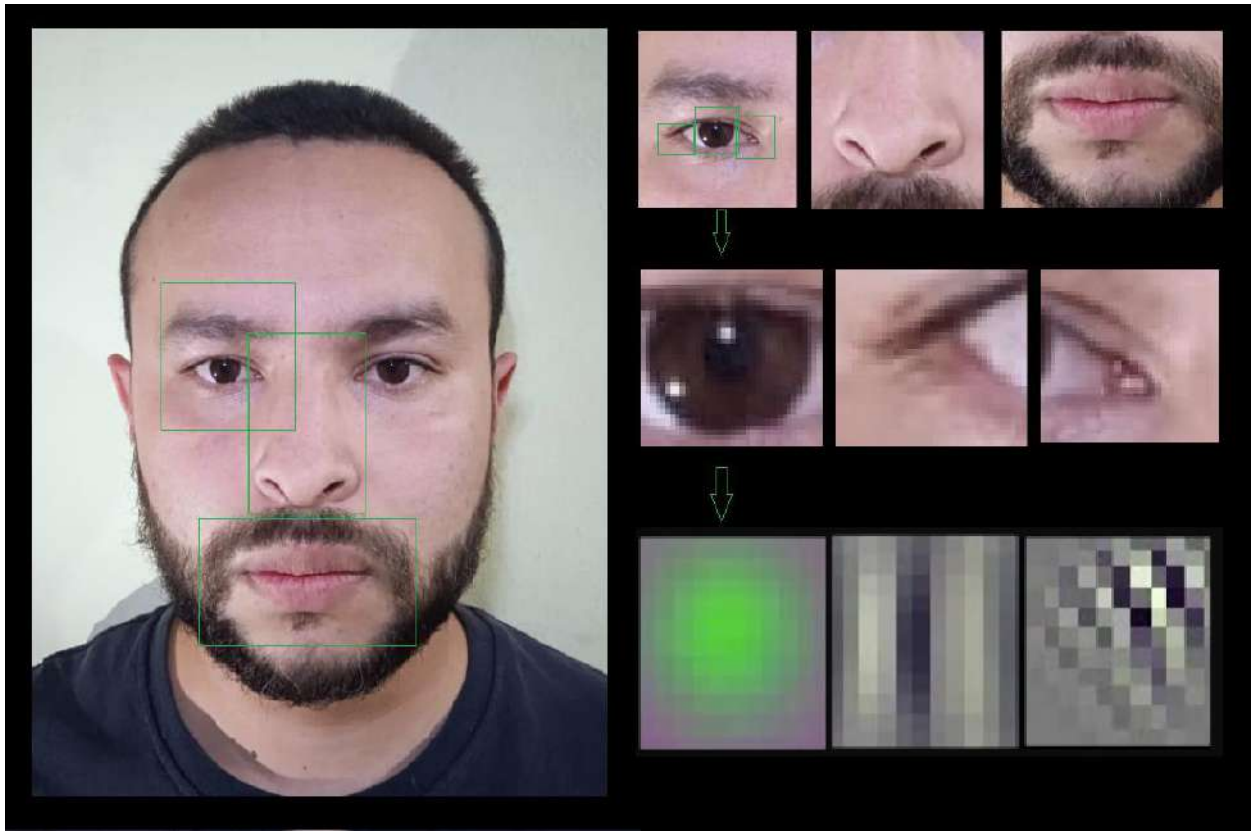
TIPOS DE INTELIGENCIA ARTIFICIAL

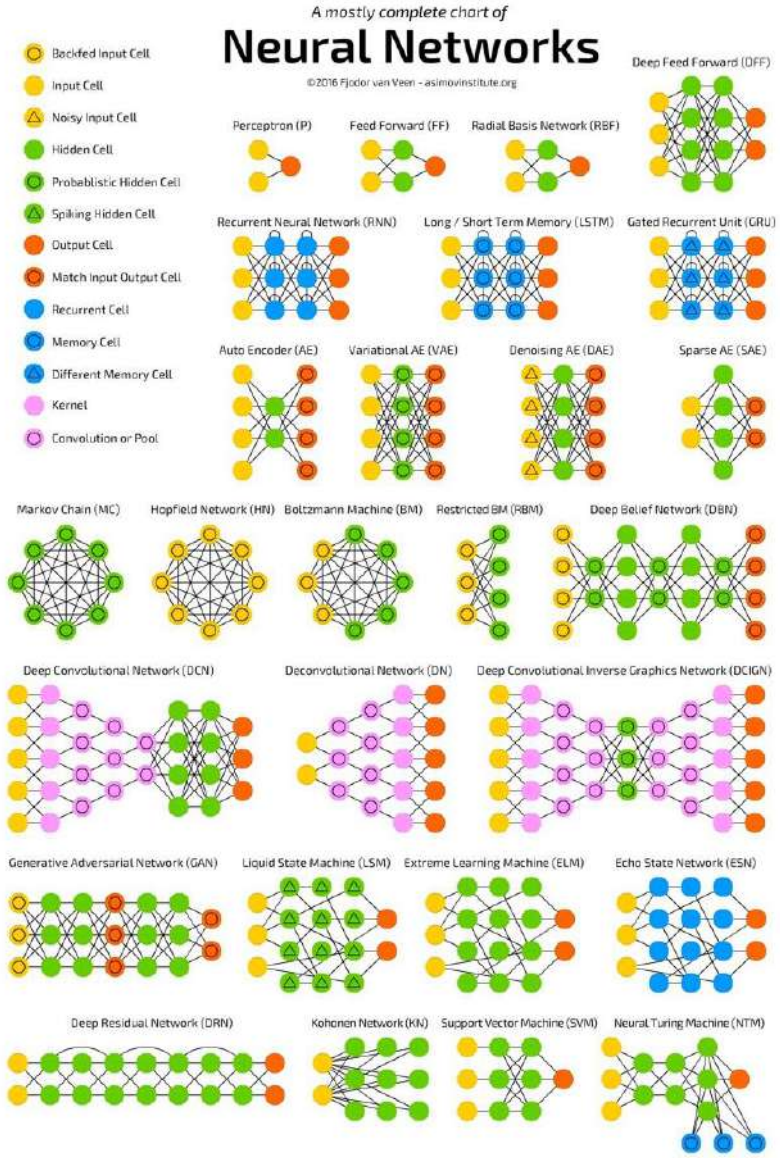


https://chatbot.fail/

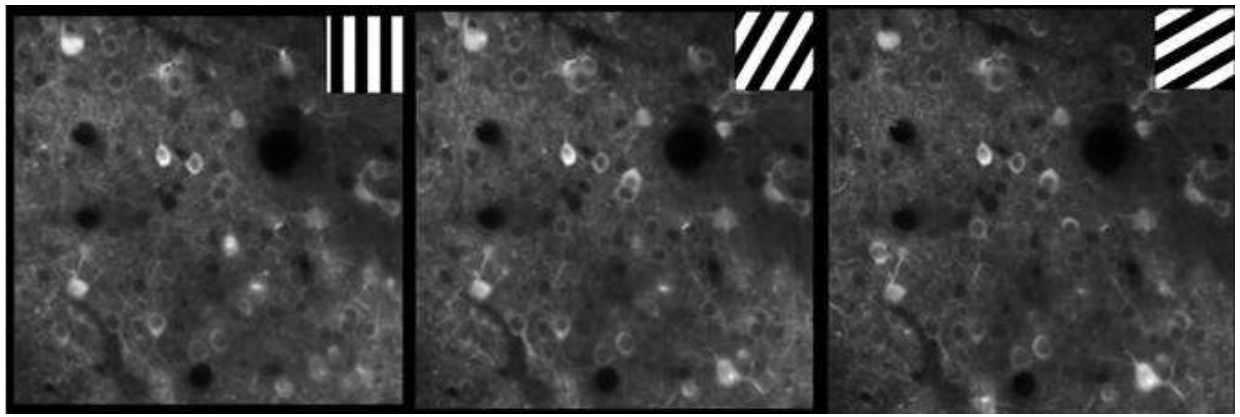
strong AI vs weak AI

MACHINE LEARNING

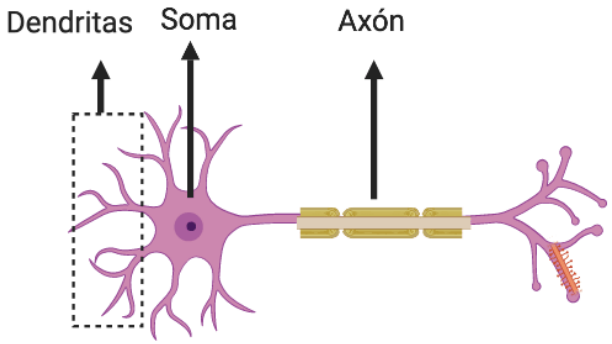


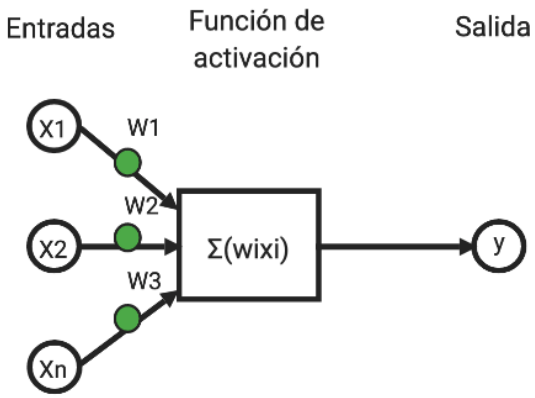


REDES CONVOLUCIONALES

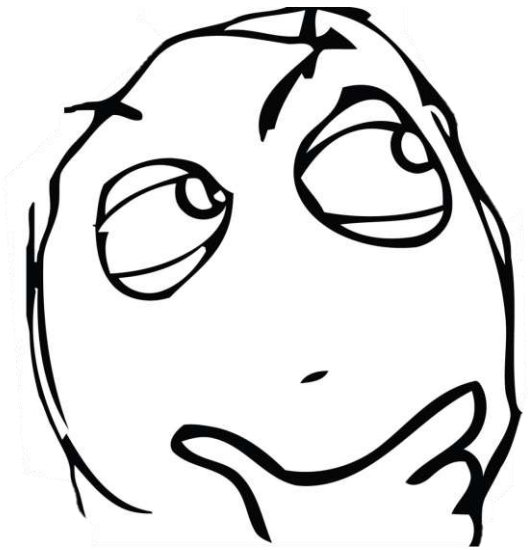


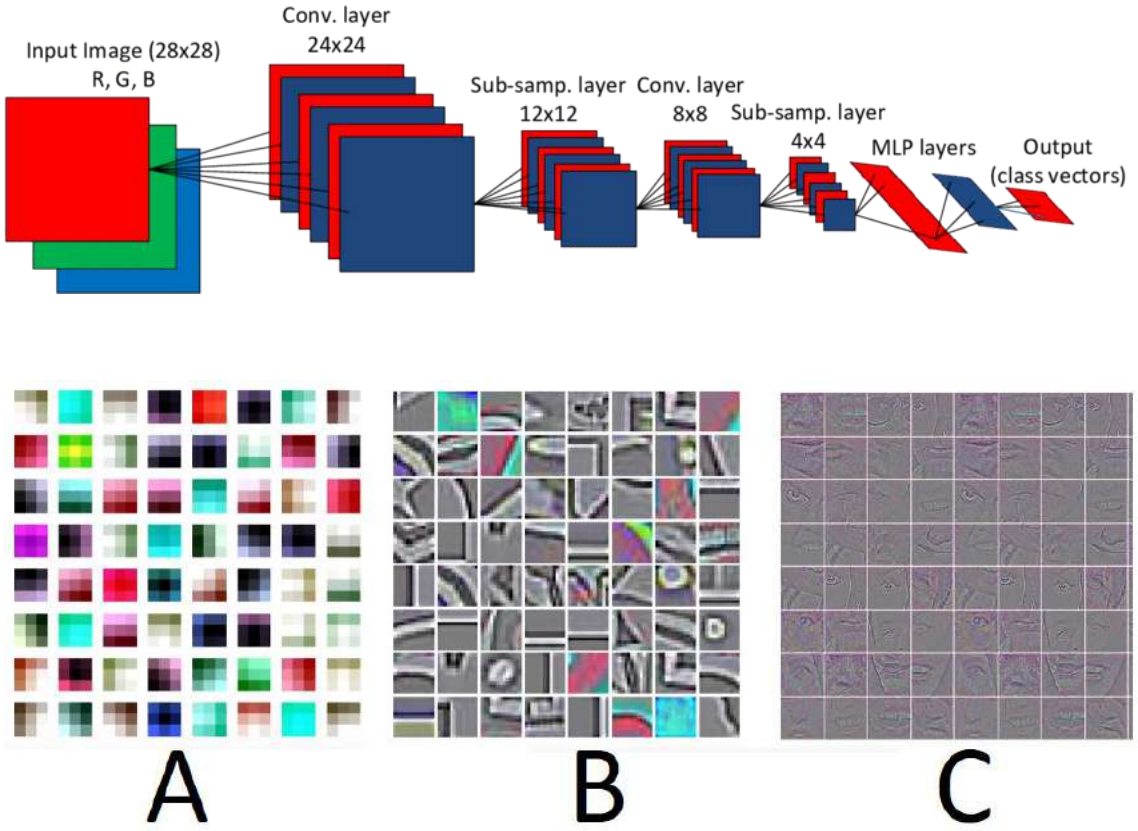
Yann Le Cun





REDES CONVOLUCIONALES





MODELOS DE INTELIGENCIA ARTIFICIAL

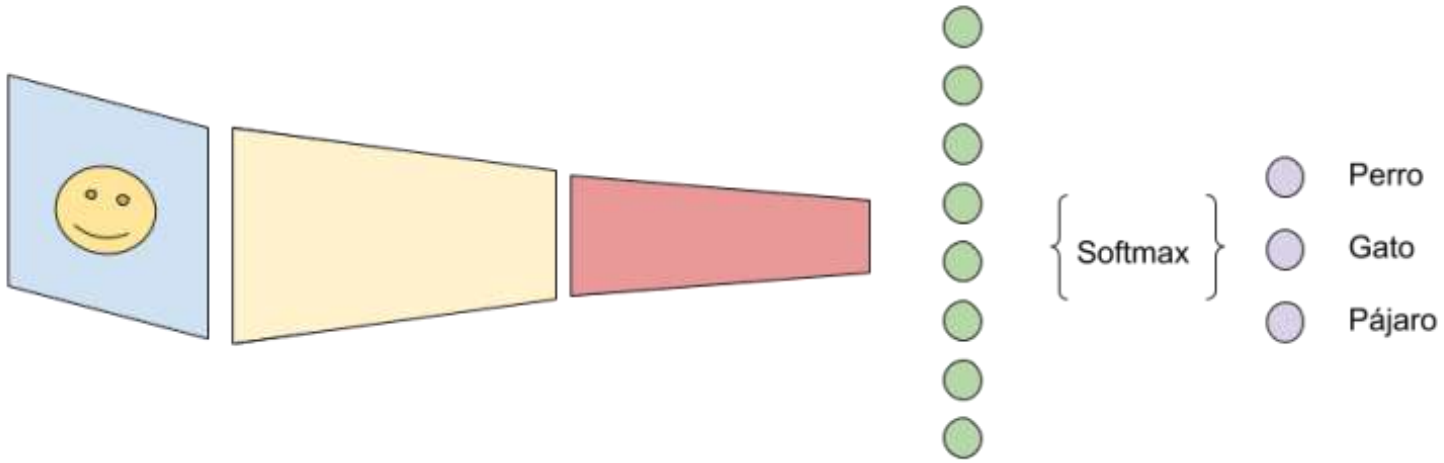


IMAGEN DE ENTRADA

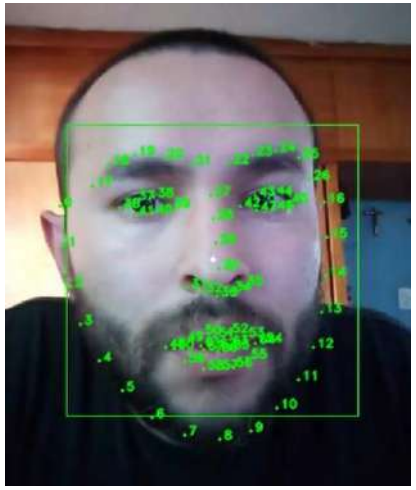
1er CONVOLUCIÓN
- FILTROS
- RELU
- SUBSAMPLING

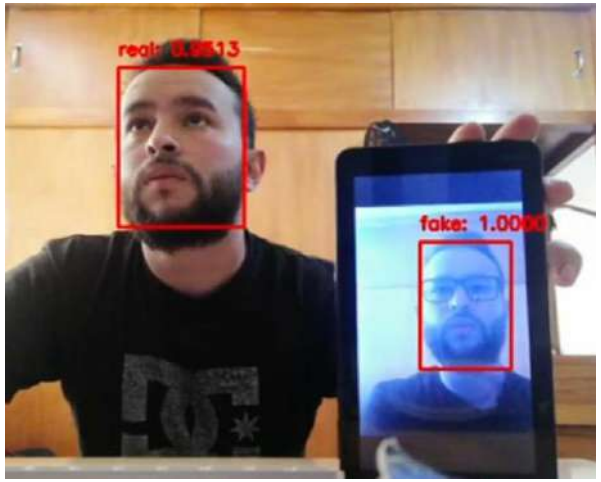
2ª CONVOLUCIÓN (Y SUCESIVAS)

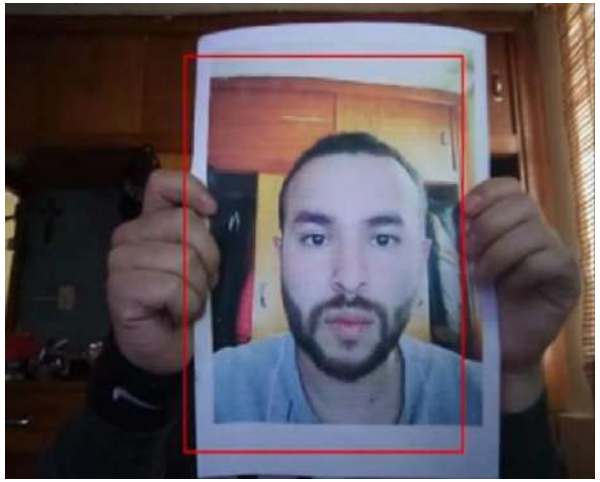
RED NEURONAL MULTICAPA (fully connected)

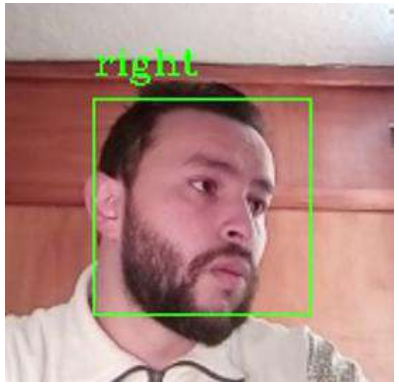
CAPA DE SALIDA: CLASIFICACIÓN ONE-HOT ENCODED

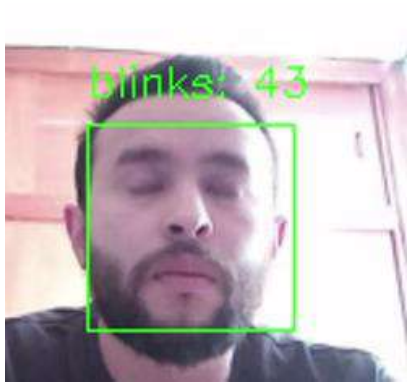
MODELOS DE INTELIGENCIA ARTIFICIAL

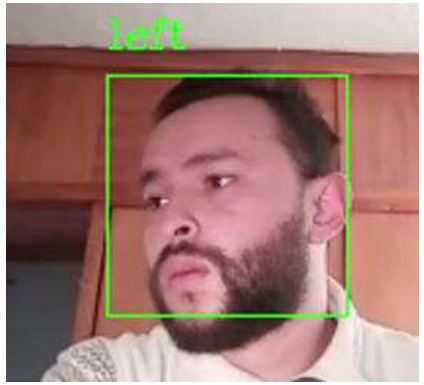




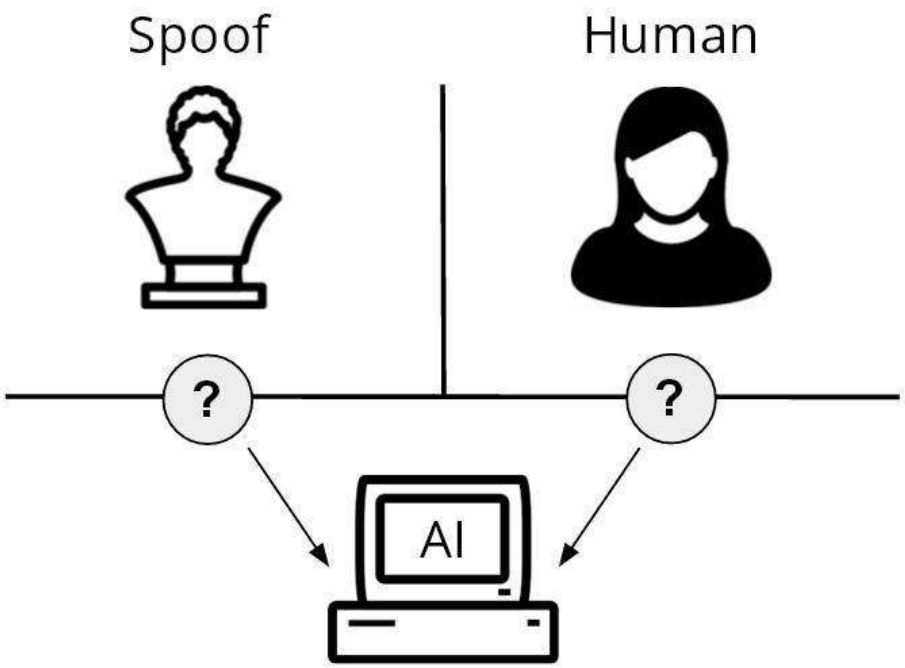








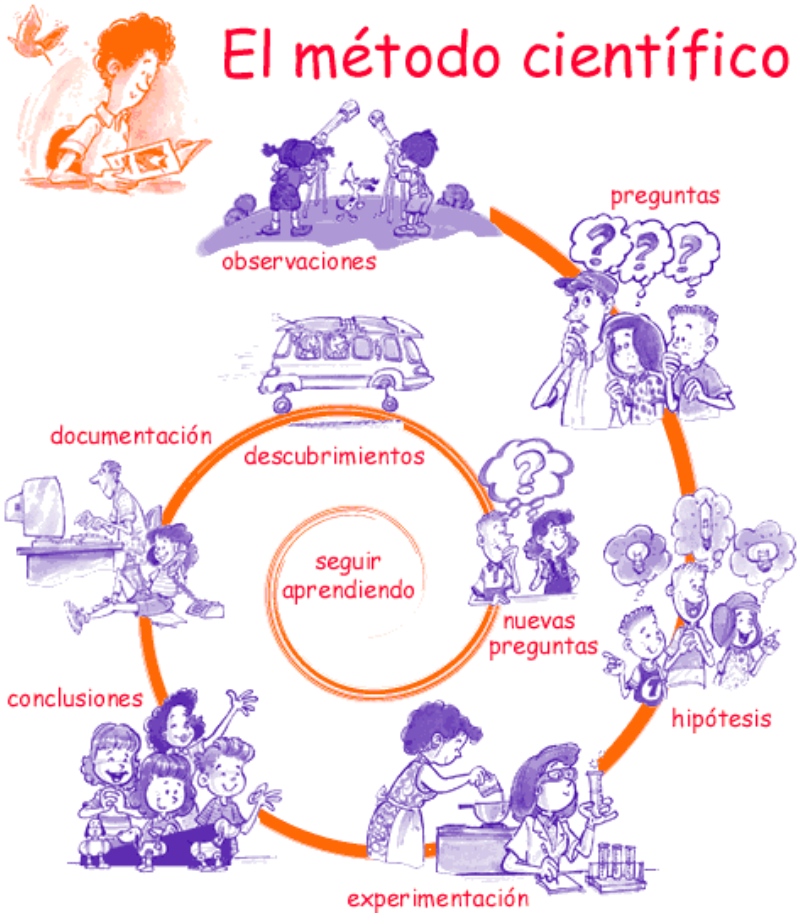
PRUEBA DE VIDA



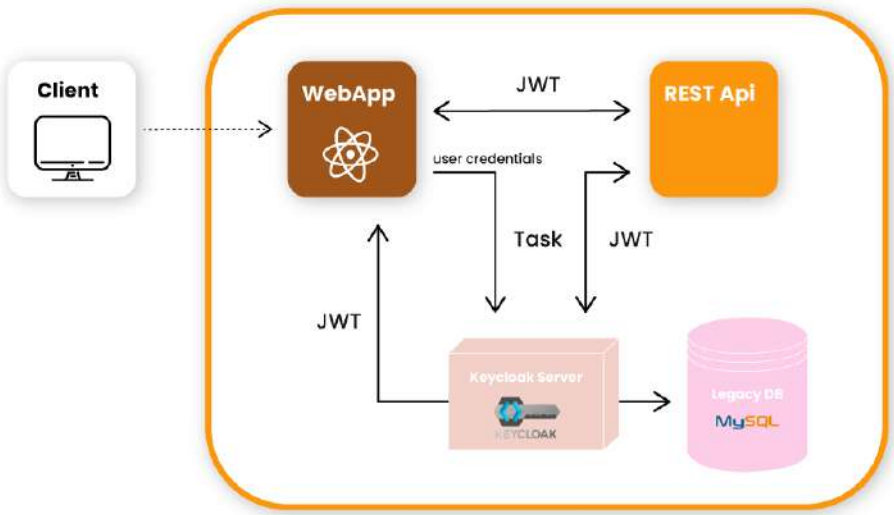
Tipo de artefacto	Descripción	Ejemplo
Nivel 1 (A)	Fotos digitales y en papel de alta resolución, videos de desafío / respuesta de alta definición y máscaras de papel.	
Nivel 2 (B)	Muñecos realistas disponibles comercialmente y máscaras 3D de resina, látex y silicona usadas por humanos con un precio inferior a $ 300.	
Nivel 3 (C)	Máscaras 3D ultrarrealistas hechas a medida, cabezas de cera, etc., con un costo de creación de hasta $ 3,000.	

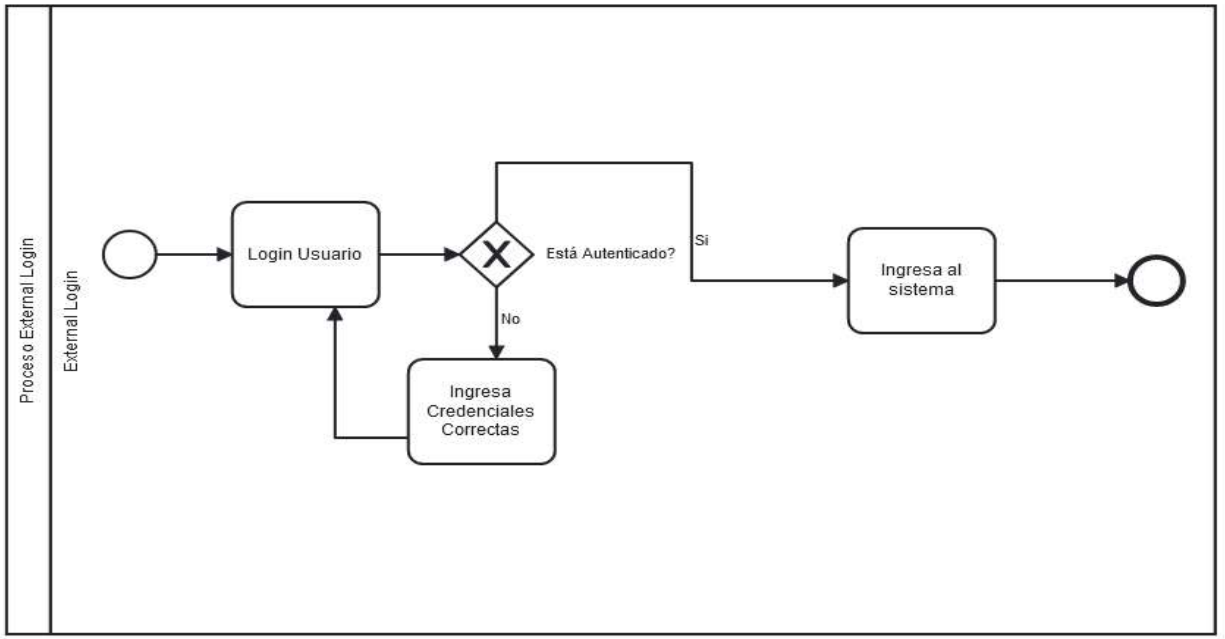
Tipo de derivación	Descripción	Ejemplo
Nivel 4	Descifre y edite el contenido de un 3D facemap ™ para que contenga datos sintéticos no recopilados de la sesión, haga que el servidor procese y responda con Liveness Success.	
Nivel 5	Toma el control de la alimentación de la cámara e inyecta fotogramas de video capturados previamente o una marioneta falsa que da como resultado que facetec AI responda con "Liveness Success".	

METODOLOGÍA

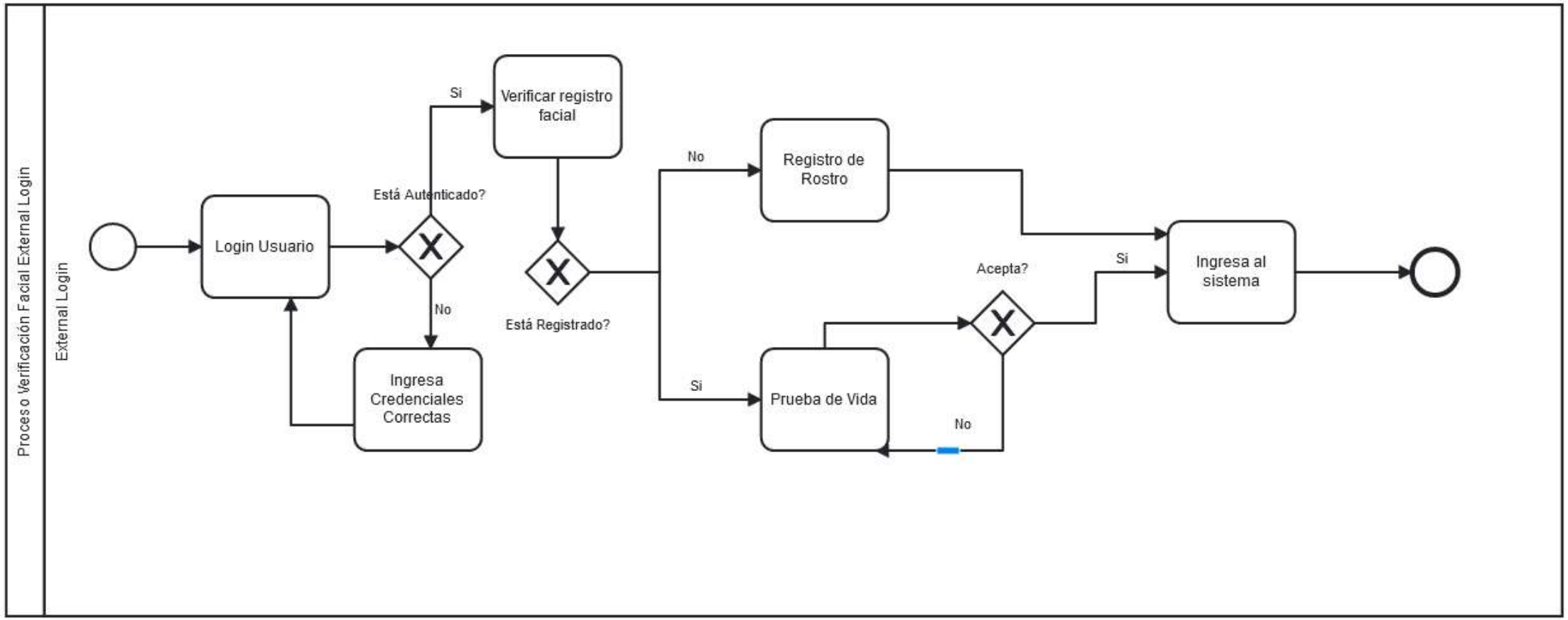


PUNTO DE PARTIDA

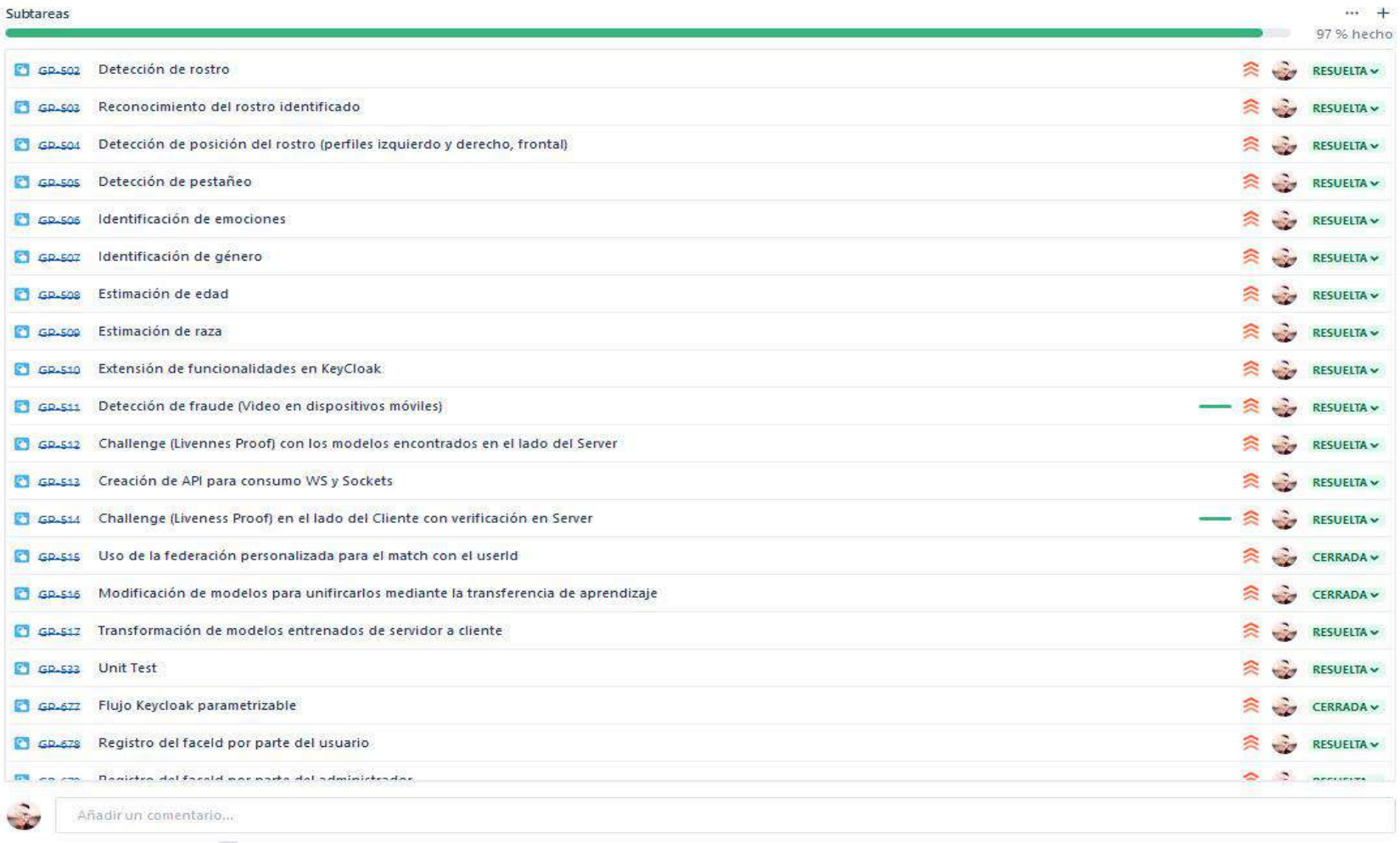




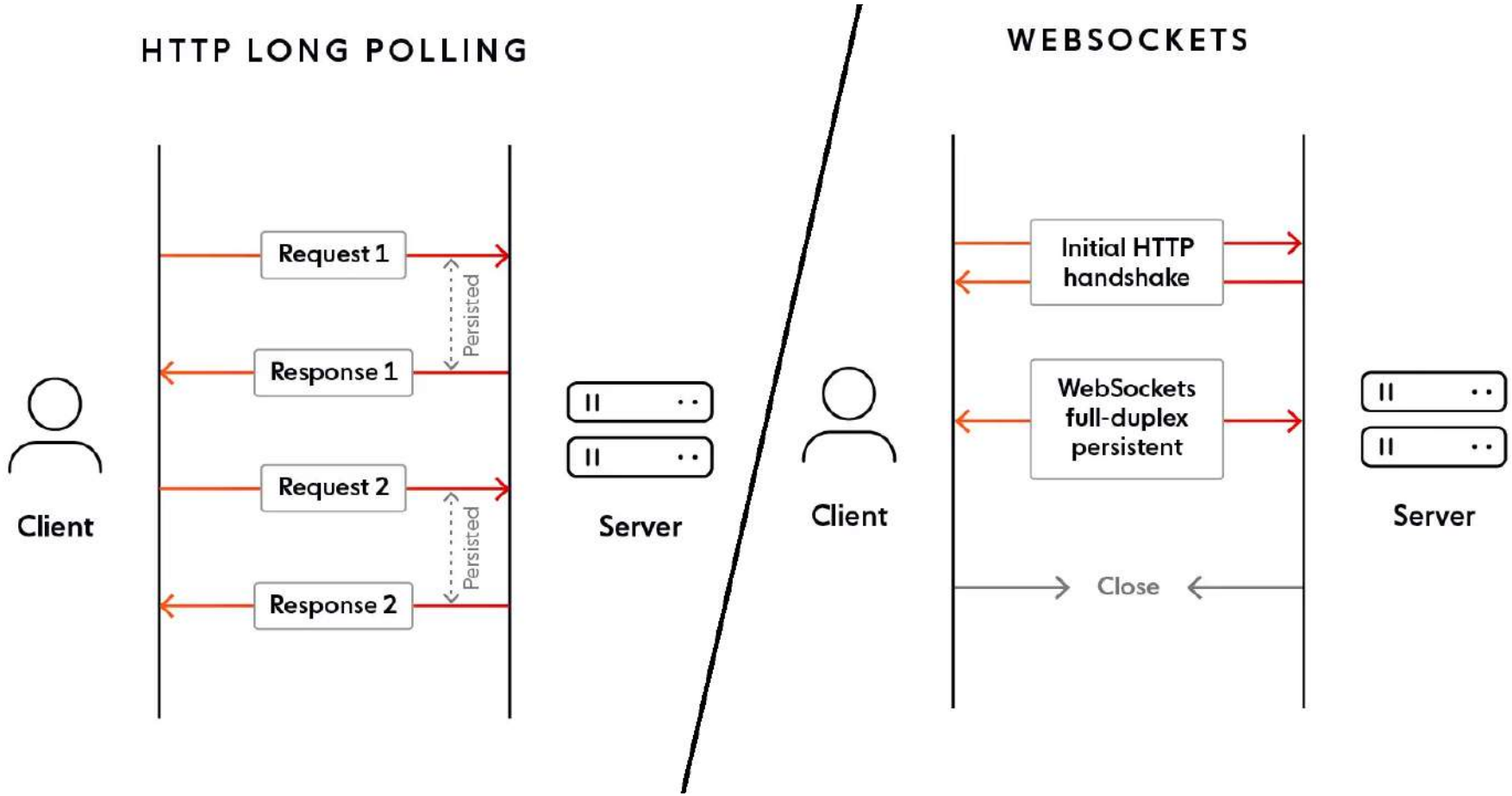
PUNTO OBJETIVO



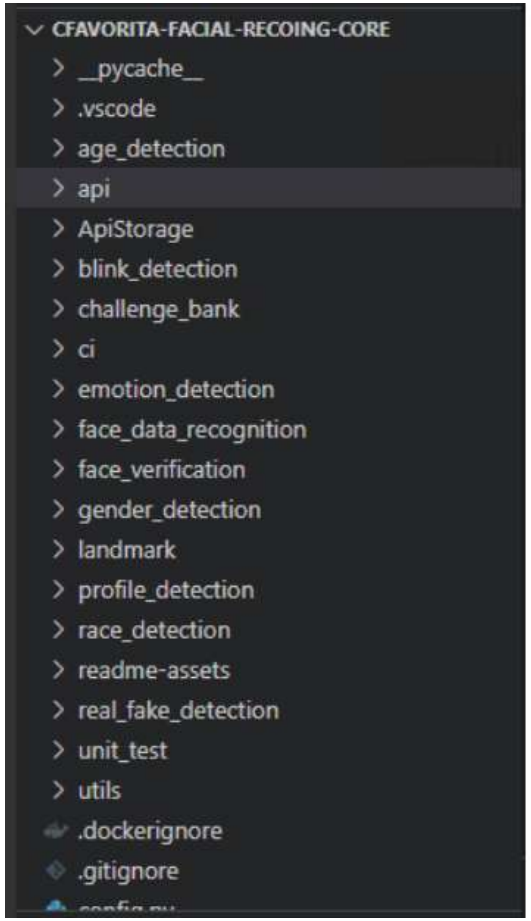
DESARROLLO DEL SISTEMA

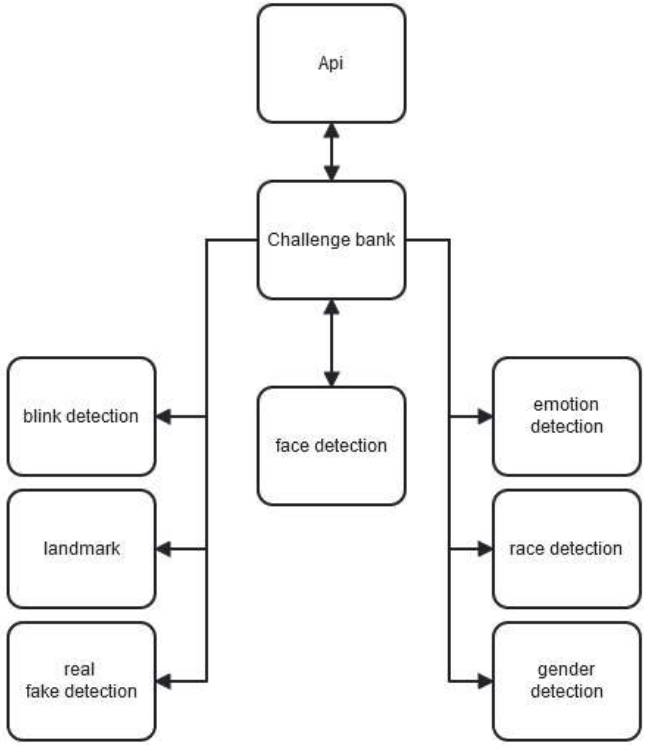


PROTOCOLO DE COMUNICACIÓN

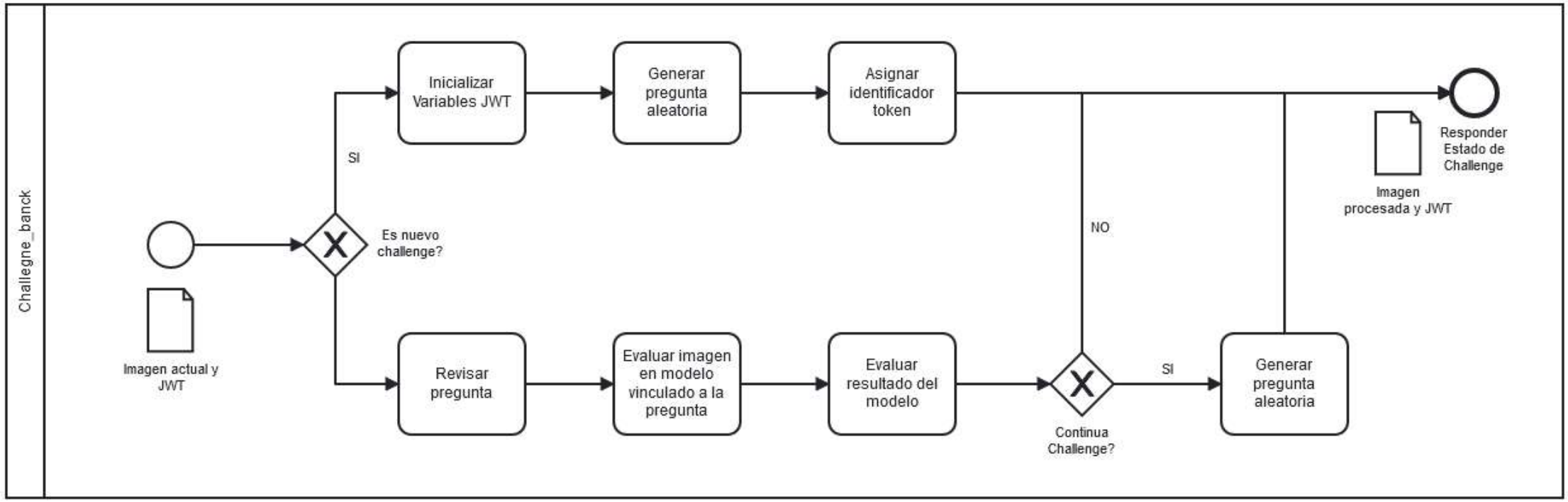


ARQUITECTURA

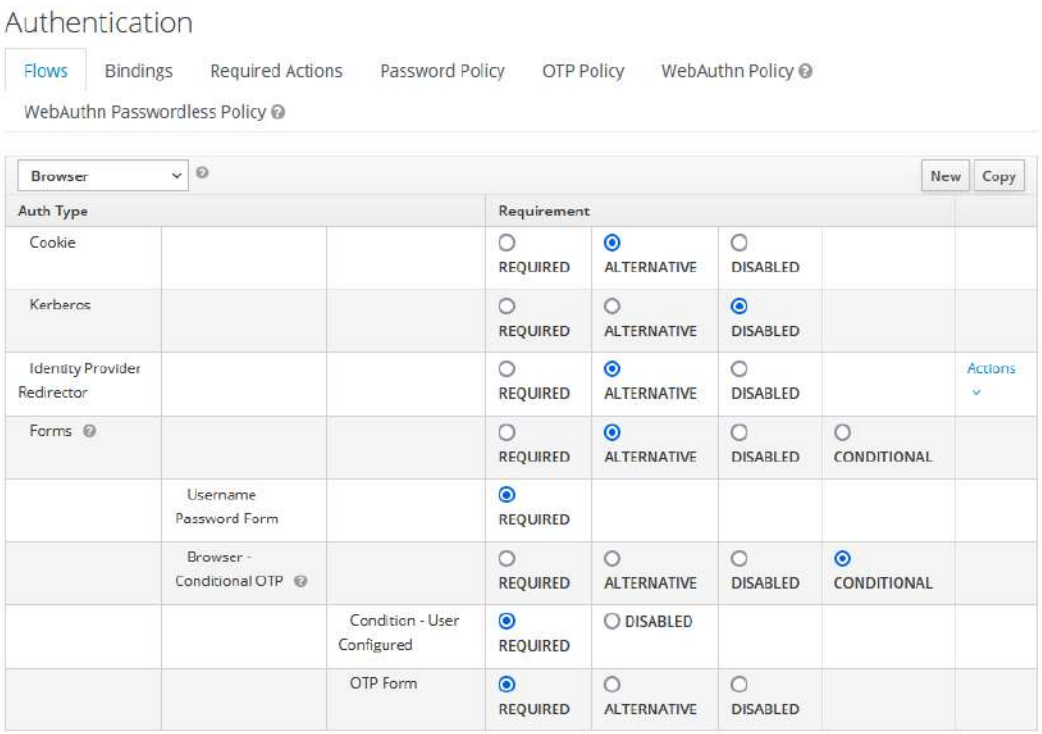


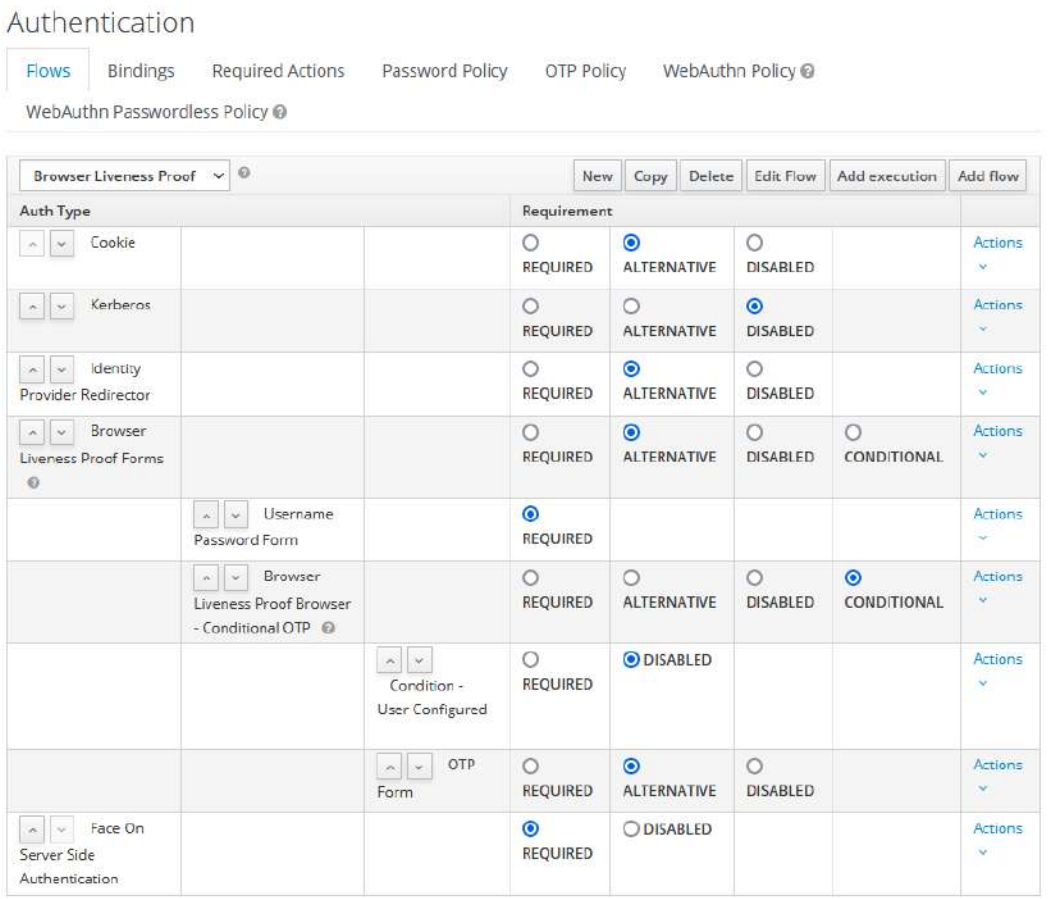


BANCO DE PREGUNTAS

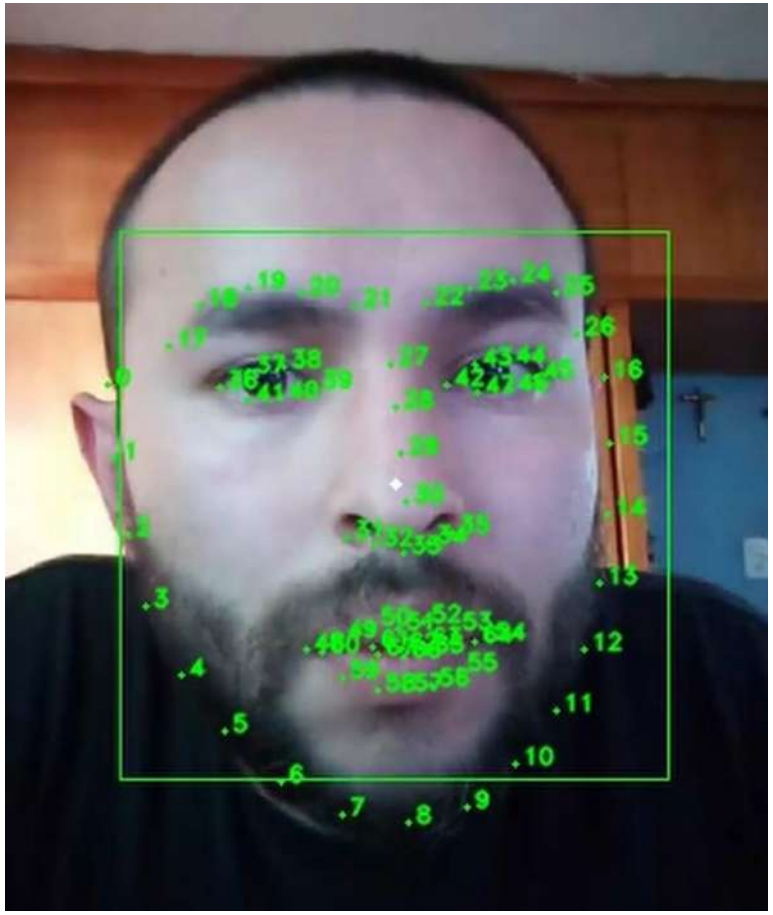


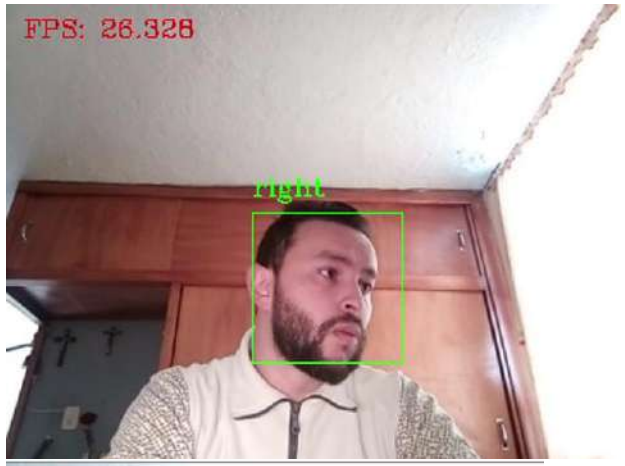
EXTENDER FUNCIONALIDADES DE KEYCLOAK

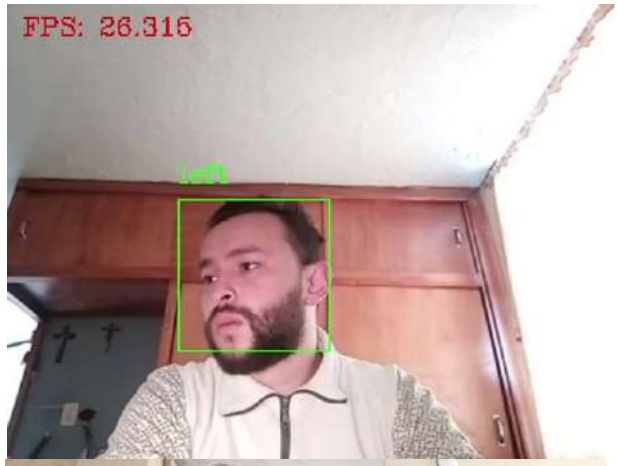


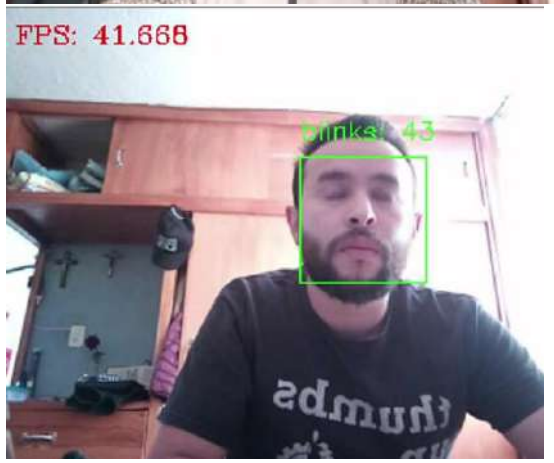


MODELOS ACEPTADOS

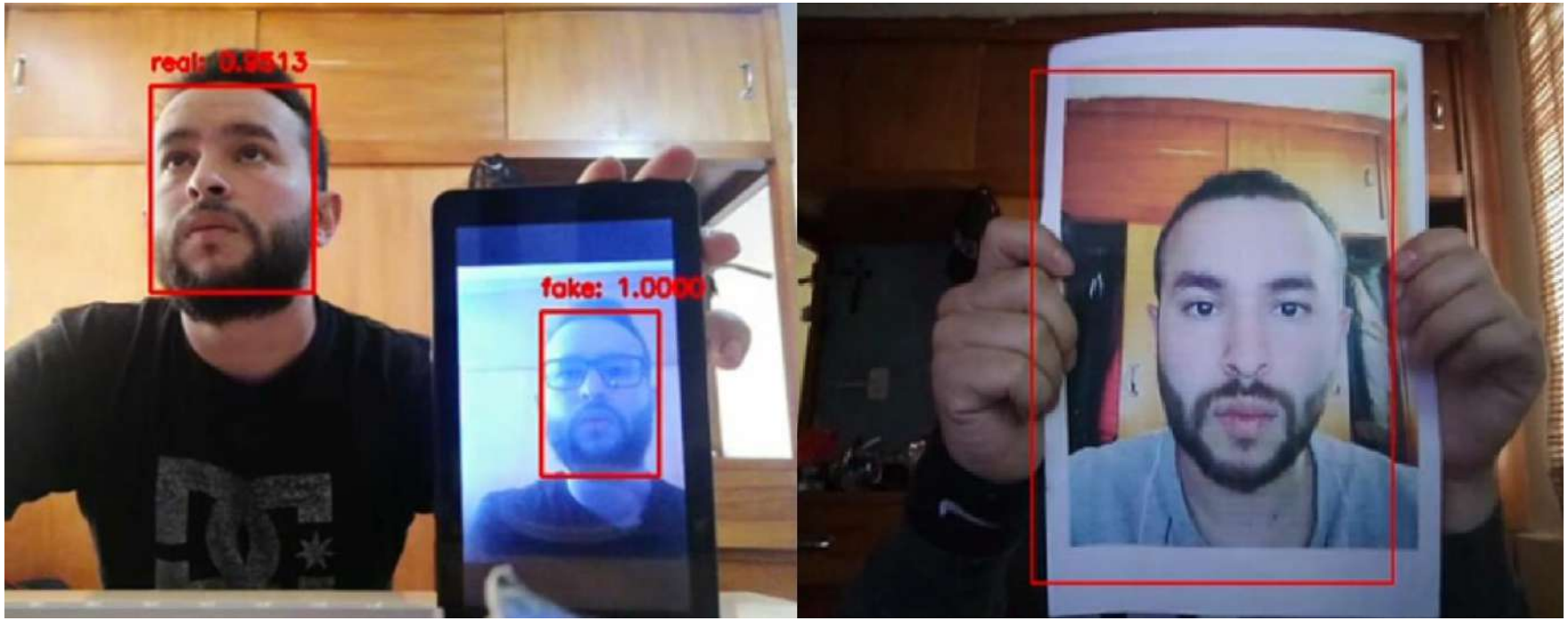




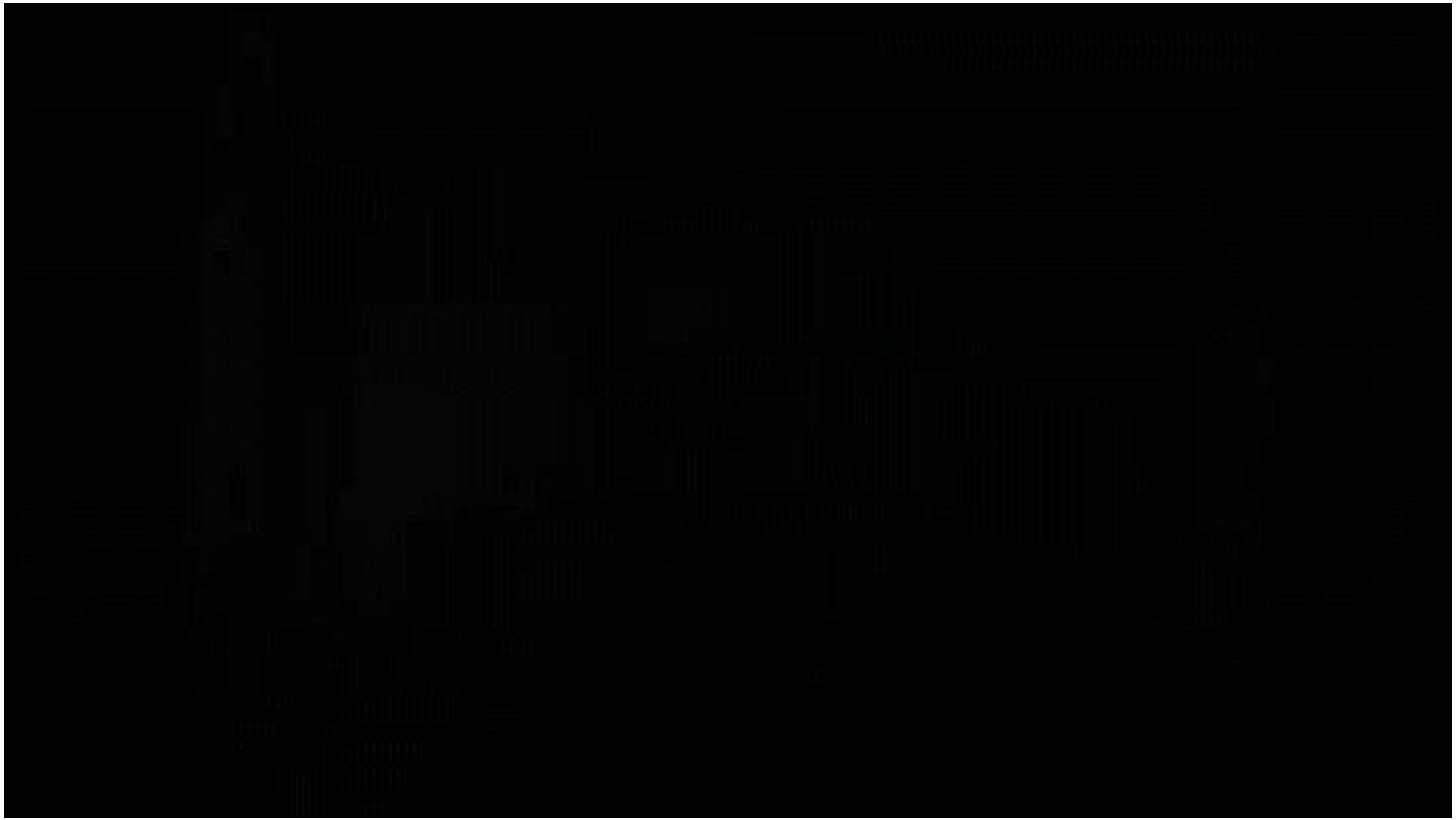




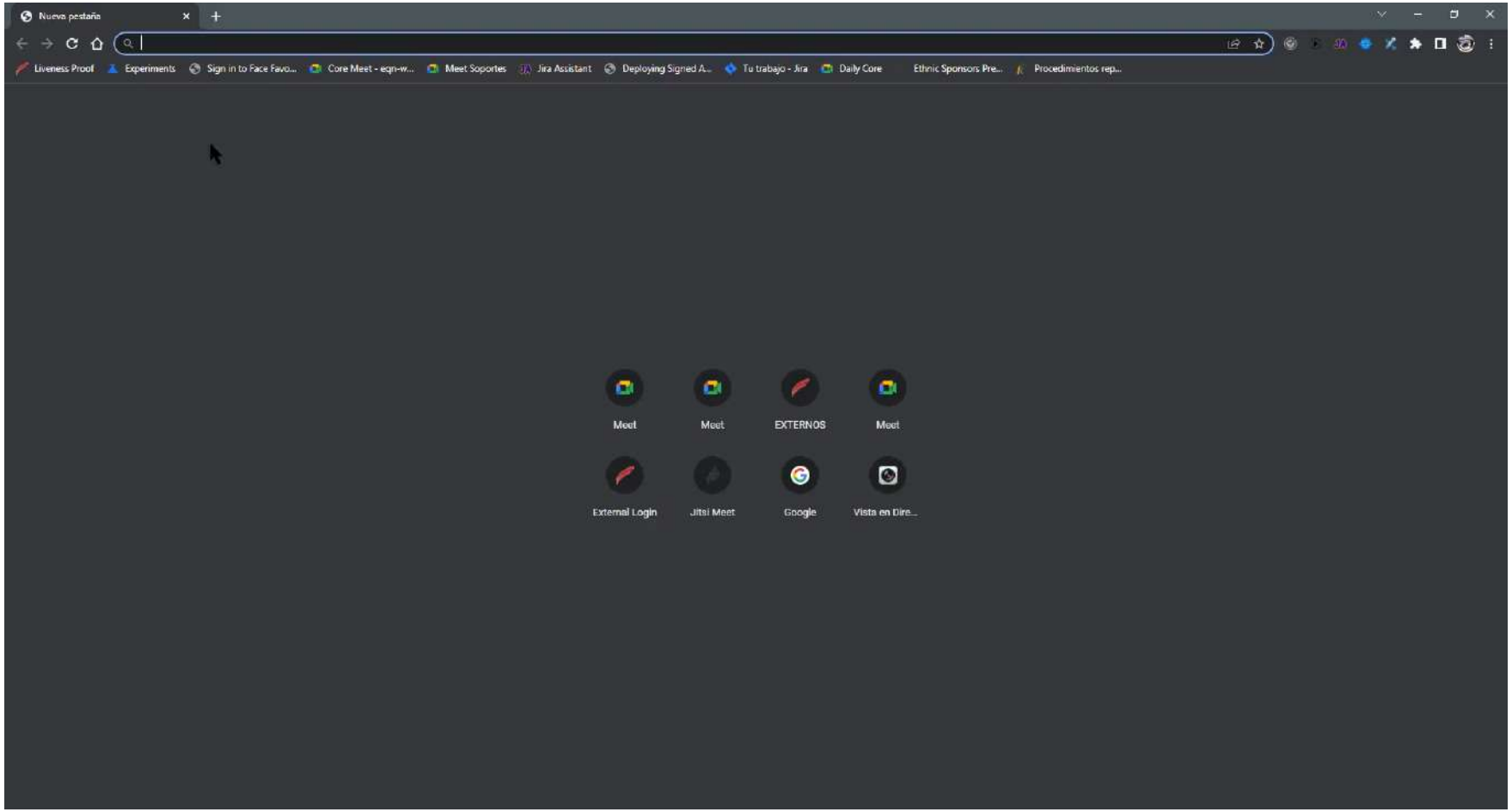
MODELOS DESCARTADOS



PRUEBAS DE MODELOS



SISTEMA EN PREPRODUCCIÓN



CONCLUSIONES

No se encontró diferencia significativa entre los modelos de detección de rostro, por lo cual, la utilización de cualquiera de los mencionados en este documento puede ser sostenible para la solución propuesta.

La mejor opción fue utilizar una comunicación websocket bidireccional entre el cliente y el servidor, ya que la propuesta de solución requería un canal de comunicación en tiempo real.

La solución propuesta fue diseñada para integrarse correctamente al proveedor de identidades keycloak.

RECOMENDACIONES

Para integrar diferentes modelos de inteligencia artificial hay que tener en cuenta la forma peculiar de utilizar cada uno de esos modelos, y estandarizar el consumo usando patrones estructurales como el Adapter que permite la colaboración entre objetos con interfaces incompatibles.

Para una efectiva ejecución de la solución propuesta en este documento se recomienda la utilización de hardware acelerado por tarjetas gráficas porque permiten la paralelización de las inferencias requeridas de diferentes modelos de inteligencia artificial.

GRACIAS POR SU ATENCIÓN

¿PREGUNTAS?