SAMSUNG

Samsung Innovation Campus

AI COURSE

Together for Tomorrow!
Enabling People
Education for Future Generations

WildPassPro: Generador y Validador de Contraseñas Seguras con IA.

The Wild Project.

AI COURSE

Parámetros proyecto

Team

- Presentación del equipo

Planteamiento

- Problema a resolver

Objetivos

- Meta hacia la cual se dirigen las acciones del proyecto

Herramientas

- Usadas en el desarrollo del proyecto (Arquitectura)

Demostración **(2min)**

- Breve explicación del resultado del proyecto, **en tiempo real**

Competencia

- Mejoras respecto a otras personas

Importancia y Relevancia del Proyecto

- ¿Por qué este proyecto es relevente e importante para la comunidad? ¿Qué les hizo querer desarrollar esta aplicación?

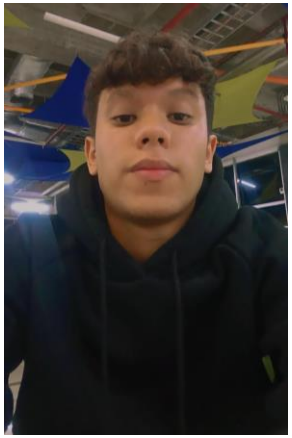
5

MINUTOS

Team

Anderson Perdomo
andersonjperdomo@gmail.com

Como líder de este equipo me encargo de que el trabajo se haga se manera ordenada, concisa y este bien estructurado para disminuir el porcentaje de error.



Diergo Alviarez
dilanalviarez@gmail.com

Soy el segundo al mando y me encargare de apoyar al líder y a los integrantes del grupo en las tareas que realicemos, daré mis opiniones e ideas para desarrollar un buen Proyecto. Soy el encargado de realizar la pagina web

Jeremy Vicent
jeremyvicent28@gmail.com

Con todo mi esfuerzo y desempeño apoyare a mis compañeros en este proyecto. Soy el encargado de realizar el código para la limpieza del dataset.

Kevin Rodríguez
kenken29815793@gmail.com

Con todo mi esfuerzo y desempeño apoyare a mis compañeros en este proyecto. Soy el encargado de realizar el código que muestre todas las graficas basadas en estudios realizados.

Team

Greymel Moreno
greymelmoreno@gmail.com

Como integrante de este grupo, daré todo mi esfuerzo y desempeño, apoyare a mis compañeros en este proyecto. Seré el encargado de finalizar todo código que requiera información extra, para darle un toque visual más agradable al proyecto.

Planteamiento

Nuestro proyecto aborda un problema crítico en la ciberseguridad global.
Problema a resolver: La vulnerabilidad de sistemas y cuentas debido al uso de contraseñas débiles o predecibles.
Problema Global a Resolver
1. Contraseñas débiles y reutilizadas

- Según estudios (informes anuales de Verizon DBIR), más del 80% de las brechas de seguridad están vinculadas a contraseñas inseguras o robadas.
- Los usuarios suelen elegir contraseñas fáciles de recordar (como "123456", "password") o reutilizarlas en múltiples servicios, lo que las hace vulnerables a ataques de fuerza bruta, diccionario o phishing

Nuestro proyecto ofrece distintas soluciones como:
1. Generador de contraseñas basado en IA

- Usa una red neuronal entrenada con un dataset de contraseñas reales (incluyendo filtradas en brechas) para generar contraseñas fuertes pero memorables.
- Evita patrones comunes (secuencias numéricas) y prioriza combinaciones poco predecibles pero factibles para humanos.
- Impacto global:
- Reduce el uso de contraseñas débiles y la dependencia de usuarios a prácticas inseguras.

Planteamiento

2. Validador inteligente de fortaleza

- Analiza la contraseña en contexto (ej. similitud con contraseñas filtradas, patrones geográficos o culturales, secuencias lógicas).
- La red neuronal detecta riesgos que un algoritmo tradicional (como el "zxcvbn" de Dropbox) podría pasar por alto.
- Impacto global:
- Protege sistemas al bloquear contraseñas que parecen "válidas" bajo reglas simples pero son altamente vulnerables.

Objetivos

El objetivo principal de nuestro proyecto es mejorar la seguridad cibernética a nivel global mediante la creación y validación de contraseñas robustas, utilizando inteligencia artificial para superar las limitaciones de los métodos tradicionales.

Tenemos como objetivo principal d iseñar un sistema basado en redes neuronales que genere y valide contraseñas seguras, reduciendo el riesgo de brechas de seguridad causadas por contraseñas débiles o predecibles.

Nuestras metas son:

1. Generar contraseñas fuertes y memorables.
2. Validar contraseñas con precisión contextual.
3. Reducir la dependencia de prácticas inseguras.
4. Educar a los usuarios indirectamente.

Y esperamos resultados:

- Técnicos: Un modelo de IA capaz de detectar el 95% de contraseñas débiles (comparado con el 70-80% de validadores tradicionales).
- Sociales/Ciberseguridad: Reducción del 30-50% en el uso de contraseñas vulnerables en sistemas que implementen la herramienta.

Herramientas

1. Frontend & Interfaz de Usuario
- Streamlit (import streamlit as st):
- Framework para crear la interfaz web interactiva.

2. Modelo de IA y Procesamiento
- TensorFlow/Keras
- Red neuronal secuencial con capas densas, dropout y batch normalization.
- Arquitectura: 8 nodos de entrada → 64 → 32 → 16 → 3 nodos de salida (débil/media/fuerte).
- Scikit-learn
- Preprocesamiento de datos (LabelEncoder) y división train-test (train_test_split).

3. Seguridad y Cifrado
- Cryptography (from cryptography.fernet):
- Cifrado AES mediante Fernet para proteger el archivo de contraseñas.
- Secrets (import secrets):
- Generación criptográfica segura de contraseñas y tokens.
- Hashlib (import hashlib):
- Verificación de contraseñas comprometidas usando SHA-1

4. APIs Externas
- Groq API
- Usa el modelo Llama3-70B para análisis avanzado de contraseñas y explicaciones de vulnerabilidades.
- Requests (import requests):
- Consultas a APIs externas (ej. descarga de rockyou.txt, verificación de fugas de datos).

Herramientas

5. Gestión de Datos
- Pandas/Numpy
- Carga y procesamiento del dataset de contraseñas (password_dataset_final.csv).
- RegEx
- Detección de patrones de vulnerabilidades en el escáner web (XSS, SQLi).

6. Funcionalidades Adicionales
- Joblib
- Serialización del modelo entrenado
- OS/IO
- Gestión de archivos cifrados (passwords.json.encrypted) y operaciones de I/O.

Demostración (2min)

demostracion

Competencia

Nuestro proyecto compite en un mercado con soluciones establecidas, pero tenemos ventajas únicas gracias a nuestro enfoque híbrido (IA + reglas + LLM).

Nuestros principales Competidores son

1. Generadores de navegadores (Chrome, Firefox)
2. Gestores de contraseñas (Dashlane, LastPass, 1Password)
3. Generadores especializados (Strong Password Generator, Password Generator Plus)
4. Herramientas open-source (KeePass, Bitwarden)

Estos generadores tienen muchas limitaciones como:

- usan reglas básicas.
- No verifican patrones predecibles.
- Están enfocados en almacenar contraseñas, no en generarlas con IA contextual.
- No usan modelos de IA entrenados con datasets de brechas recientes.
- No personalizan contraseñas según el contexto del usuario.
- Sin capacidad de análisis semántico.

Mientras que nuestro WildPassPro ofrece:

- Una IA que genera contraseñas memorables.
- Una red neuronal que detecta patrones culturales.
- Analiza en tiempo real con LLM para explicar vulnerabilidades en lenguaje natural.
- Poseemos un escáner web integrado para detectar riesgos en sitios donde se usan las contraseñas.
- Entrenamos con datos de la dark web para evitar contraseñas con patrones hackeados recientemente.
- Sistema de cifrado local (Fernet) para la bóveda de contraseñas, no dependiente de la nube.
- Explicaciones tipo chatbot para usuarios sin conocimientos técnicos.
- Detección de fugas de datos integrada con Have I Been Pwned.

Competencia

Las mejoras de WildPassPro vs la competencia:

Característica	Competencia	Nuestro Proyecto
Generacion de contraseñas	Aleatorias o basadas en reglas	IA + red neuronal para equilibrio seguridad/usabilidad
Validación de fortaleza	Lista estatica de contraseñas debiles	Prediccion contextual con modelo entrenado en patrones actuales
Explicaciones	Metricas tecnicas	Analisis en lenguaje natural con LLM (Groq)
Proteccion adicional	Solo contraseñas	Escaner web + detector de fugas de datos
Personalizacion	Limitada o nula	Evita patrones regionales/culturales (ej. "medellin2024")
Accesibilidad	Requieren instalacion o pago	Web-based (streamlit) + gratis

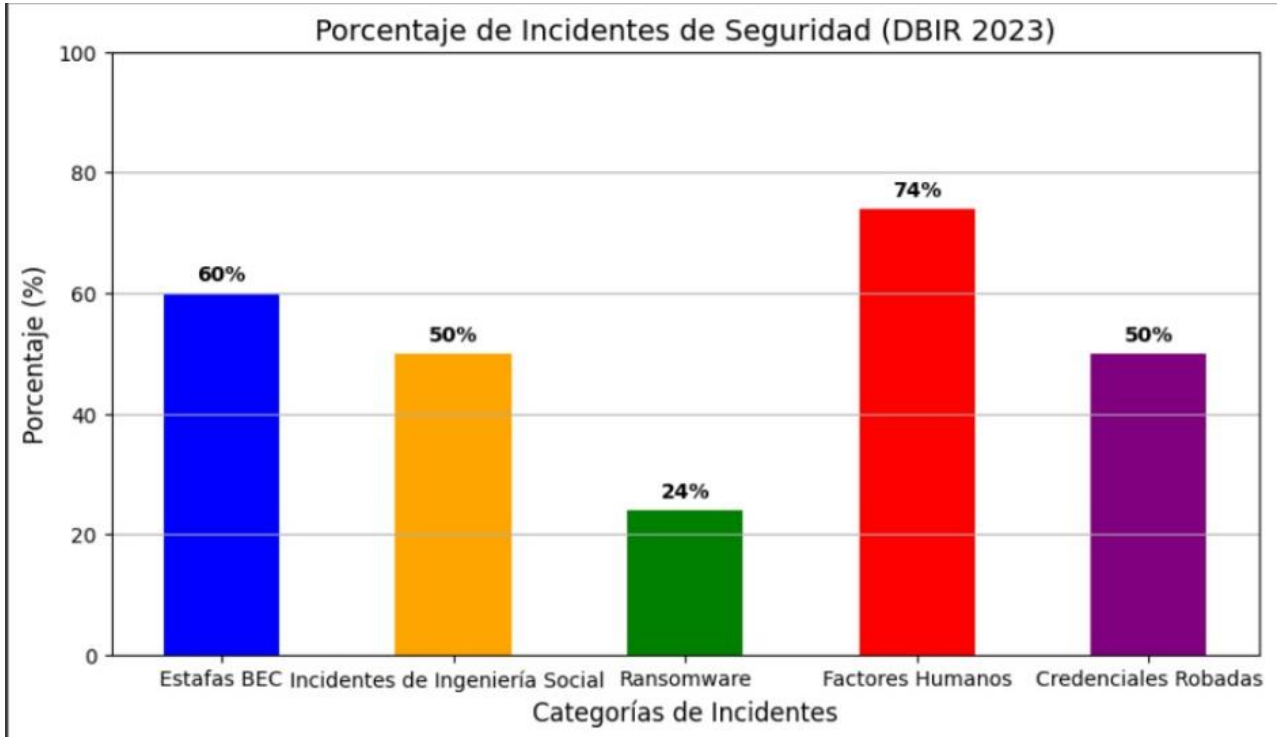
Competencia

Matriz competitiva de WildPassPro:

Característica	Navegadores	Dashlane	Generadores	Nuestro Proyecto
IA Generativa	✗	✗	✗	✓
Validación Contextual	✗	⚠	✗	✓
Bóveda Cifrada	✗	✓	✗	✓
Análisis de Vulnerab.	✗	✗	✗	✓
Explicaciones LLM	✗	✗	✗	✓
Multiplataforma	✓	✓	✗	✓ (Web)

Importancia y Relevancia del Proyecto

Nuestro proyecto es extremadamente relevante e importante para la comunidad global, responde a una crisis global de seguridad. El 81% de las brechas de datos se deben a contraseñas débiles o robadas y se estima que el 60% de los usuarios reutiliza contraseñas en múltiples plataformas, siendo esto cifras alarmantes para la seguridad cibernética ya que trae consecuencias como pérdidas económicas o riesgo para infraestructura crítica.



Nuestro proyecto mitiga esto al reducir la probabilidad de que las contraseñas sean vulnerables desde su creación.

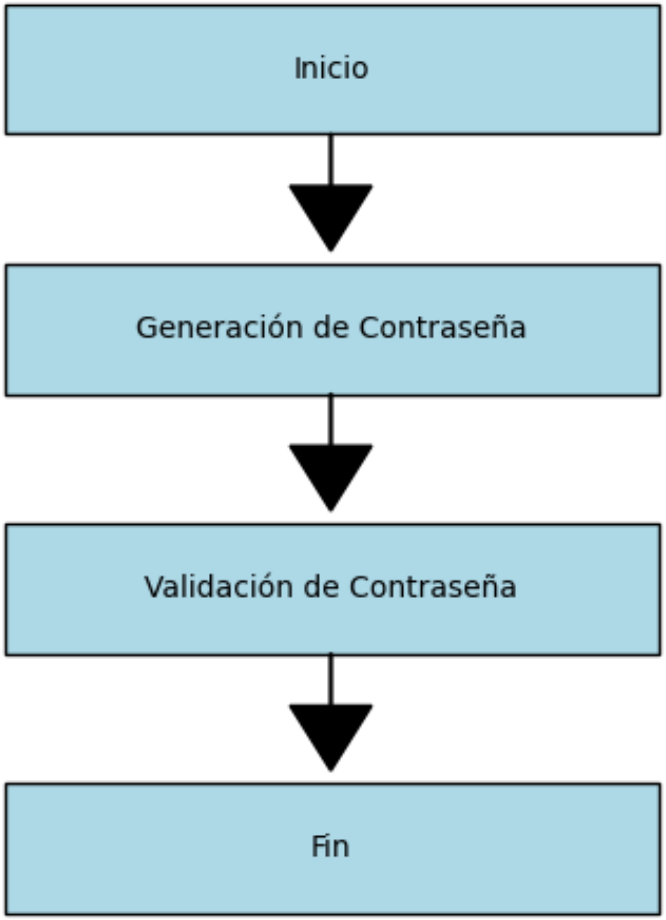
Importancia y Relevancia del Proyecto

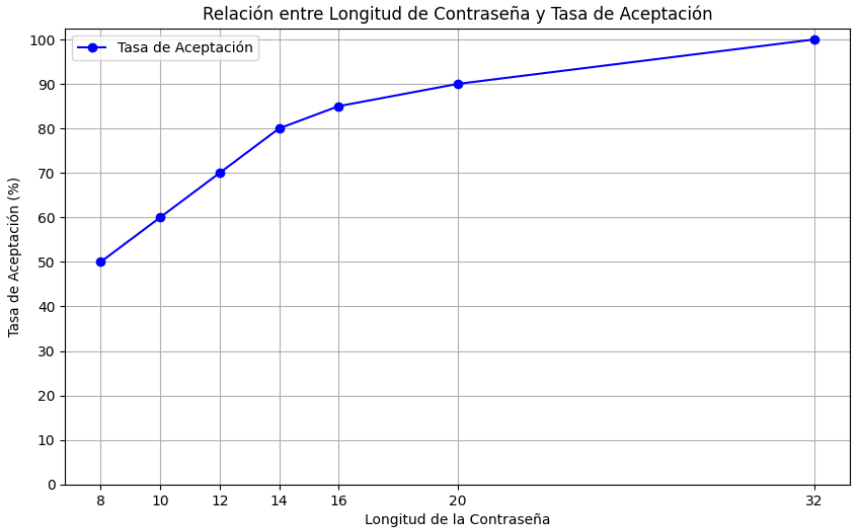
Nuestro proyecto va mas allá de solo generar una contraseña, las herramientas tradicionales solo validan la regla básica de 8 caracteres mientras que nuestro sistema analiza patrones contextuales con IA (ej. "¿Es similar a contraseñas filtradas en 2024?")

Pensamos en todo el publico que necesite y use nuestro sistema, a los usuarios no expertos les permite crear contraseñas robustas sin necesidad de entender ciberseguridad.

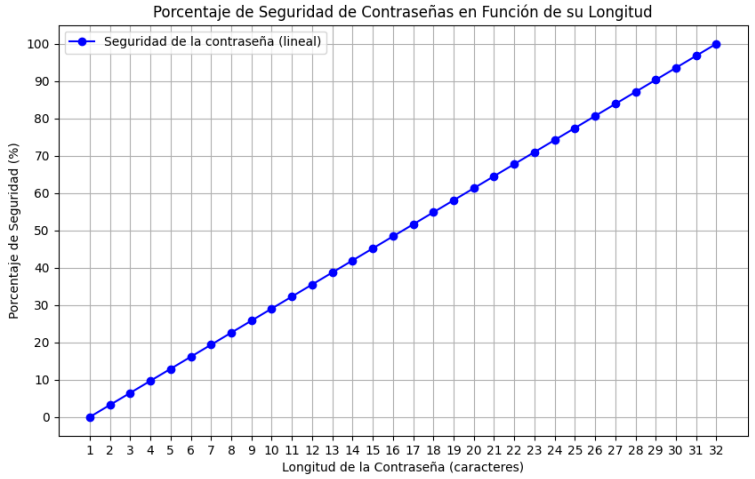
Nuestro proyecto es motivación personal, refleja una necesidad universal. Desarrollamos este proyecto porque vimos y vivimos el daño real de los ciberataques.
Este sistema prevé delitos como los robos de identidad, las extorsiones, los fraudes a niños, adultos y adultos mayores. También protegemos la privacidad evitando que fotos, mensajes o datos médicos sean expuestos y brindamos paz mental a los usuarios ya que no tendrán que recordar 50 contraseñas complejas o arriesgarse a reutilizarlas.

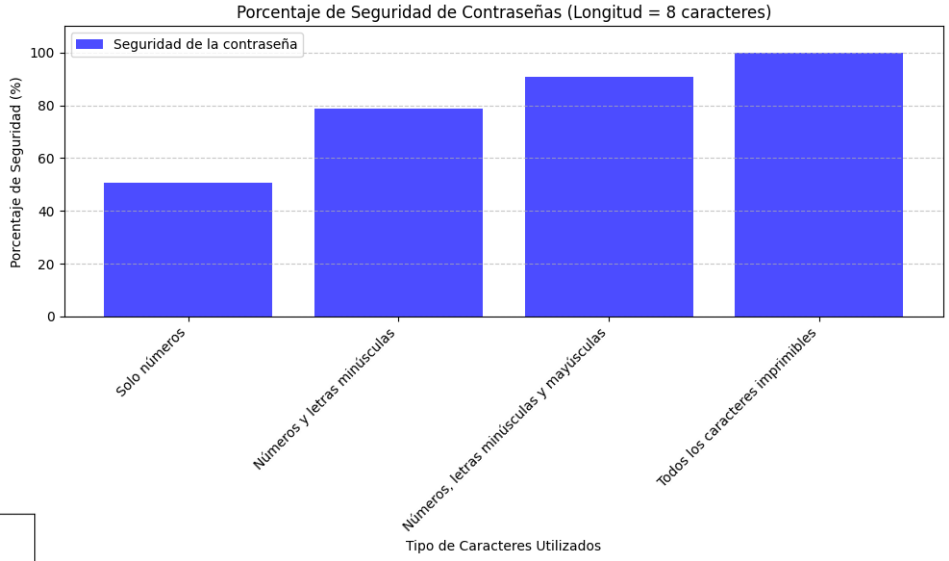
Graficas de WildPassPro

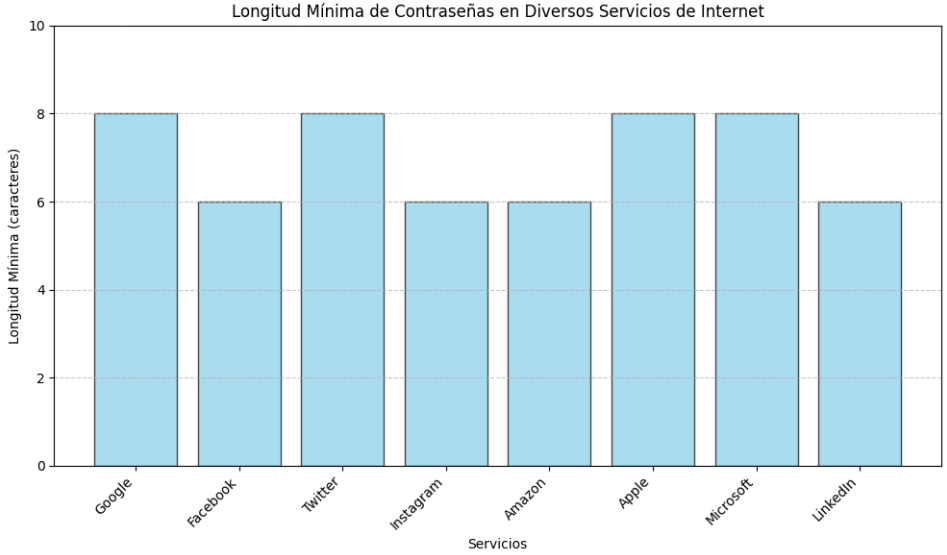




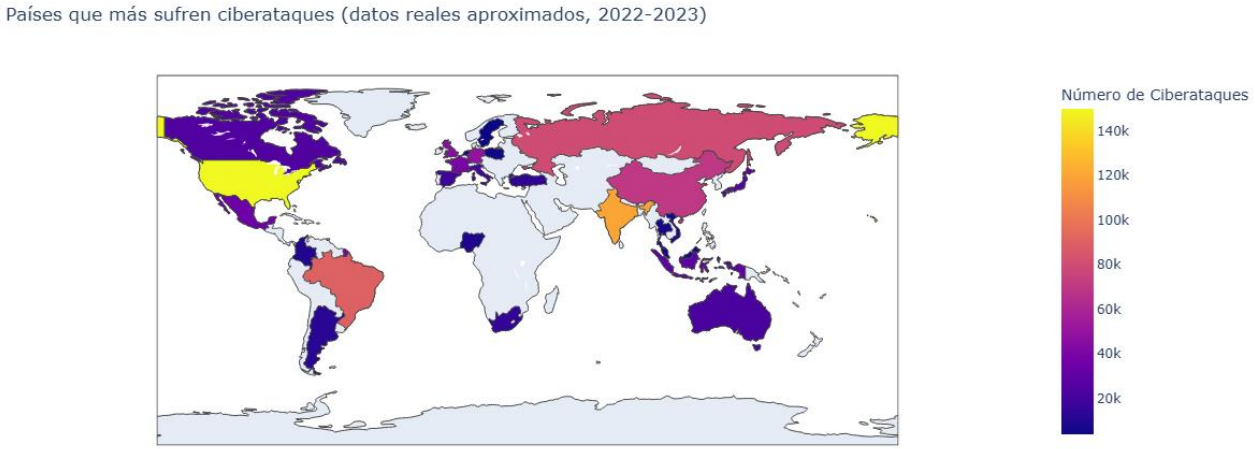
Graficas de WildPassPro

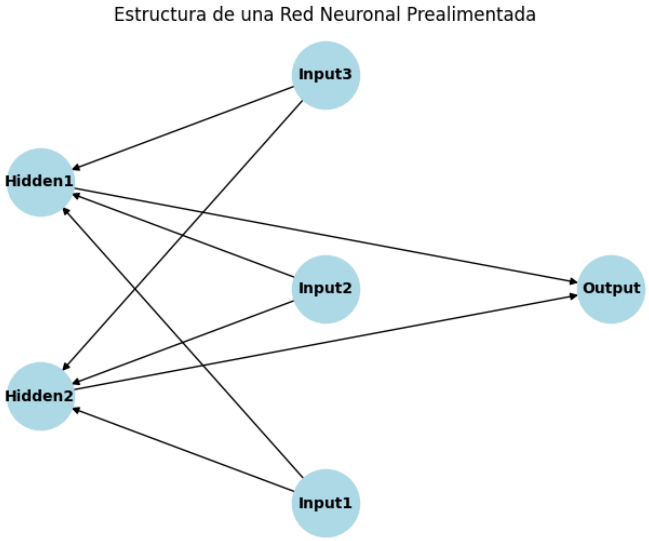


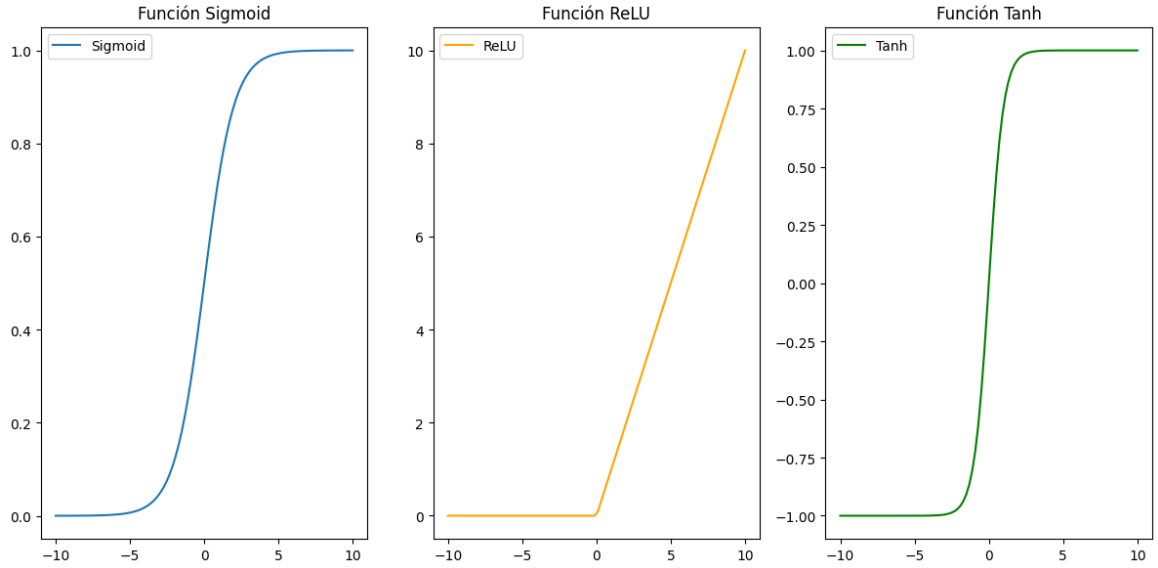




Graficas de WildPassPro







Graficas de WildPassPro