

**“Aires de Libertad”
para la Defensa Nacional**

AI Y SU IMPACTO EN LA CIBERDEFENSA

CIBERSEGURIDAD A TRAVÉS DEL TIEMPO

Jueves 31 de Agosto

11:00 AM (hora de Argentina)



José Barletta M.S.
Presidente Comité de Tecnología CAMACOL
Director de FEBICHAM
Presidente REBITI



Guillermo Otamendi
Asesor Internacional
Moderador

Ciberdefensa: activa, pasiva, proactiva, preventiva y reactiva.

Security Web Gateway • Cloud Access Security Broker (CASB)

Zero Trust Network Access (ZTNA) • WAN - LAN y MAN.

SSE y SASE • IRAM-ISO/IEC 27001 - NIST CSF



FEBICHAM
Binational Chambers of Commerce
FEDERATION



Temas a ser tratados

**Ciberseguridad a través del Tiempo.
“AI”**

Porqué es importante.

Normas existentes. Dec. Ley - Ley

Como cubrirse de Ciberataques.

Que conviene hacer.

Principales dudas. Preguntas

Recomendación --- White Paper

Mi Objetivo

Lograr **tres** cosas:



Hacer pensar



Aristóteles



Hacer sentir



Motivar



Guillermo Arduino
PRESENTA



JOSÉ L. BARLETTA, M.S.

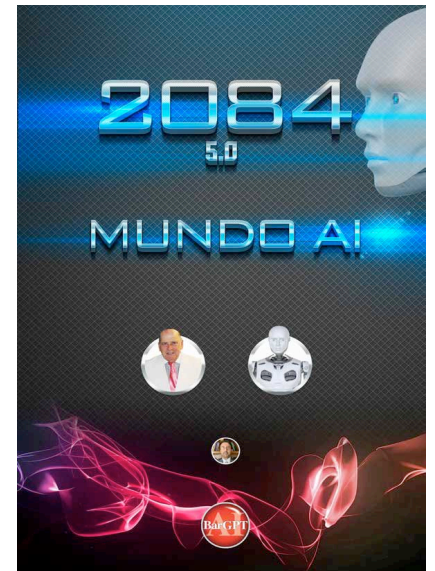
**El millennial más
antiguo de EE.UU.**



Una nueva dimensión



Libros/Eventos



GANADOR DEL PREMIO NOBEL

GABRIEL GARCÍA MÁRQUEZ



Yo no vengo
a decir un
discurso

Cambios de Paradigmas

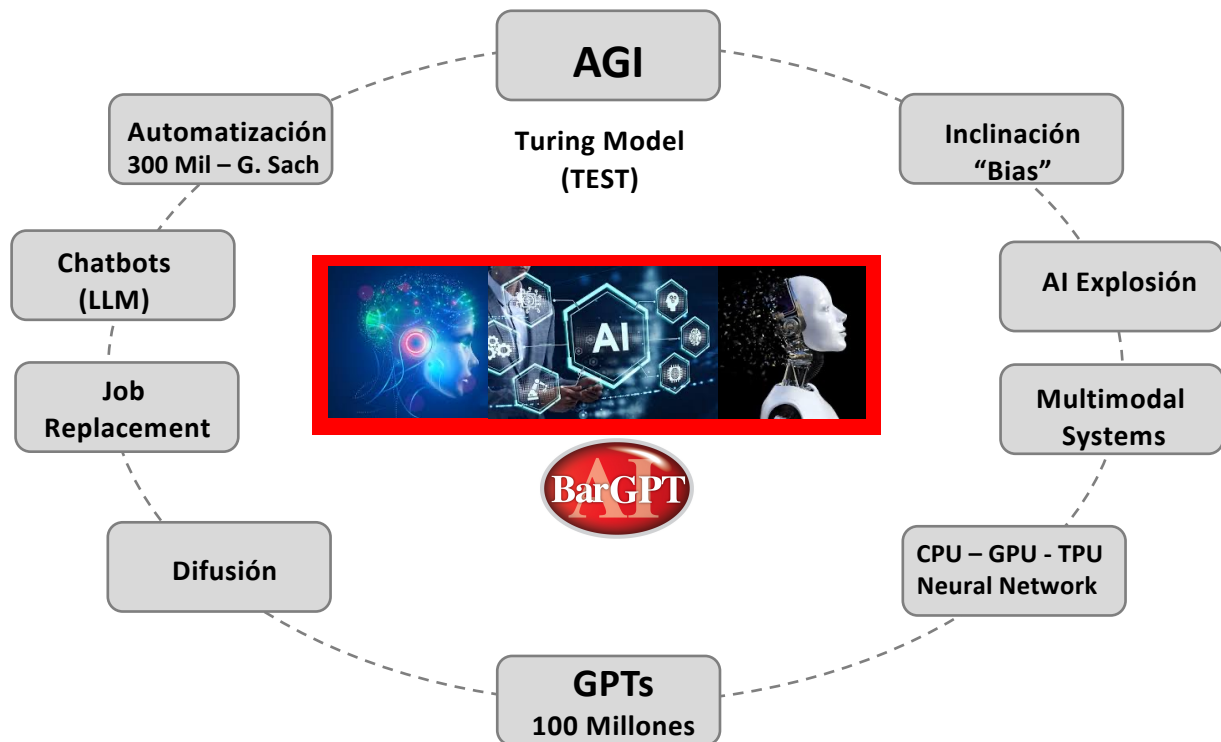


Ciberseguridad

Infocalipsis

Ciberseguridad

IA - Inteligencia Artificial



**LLM – Large Language Model
(People , Person and Facts)**

Tiempo que tardó el mundo en llegar a tener **100 millones** de usuarios:

Telefono: 75 años
iTune: 6.5 años
años Twitter: 4.5 años
Instagram: 2.5 años

Mobile phone: 16 años
Bitcoin, Facebook: 5
Whatsapp: 3.5 años
Apple App Store: 2 años

 **Chat GPT “AI”: Solo 2 Months**



Malware

Ransomware (Trojanos y spyware).

Secuestro de “DATOS”.

**Bloqueo de un dispositivo
electrónico y encriptación
de los archivos.**

Ransomware/Malware

(Software Maligno o Malicioso)

Programa que, al infectar una computadora, impide su uso normal o restringe el acceso a los documentos.

Normalmente se demanda un pago.

Ataques Cibernéticos

1. Malware

2. Virus

3. Gusanos

4. Troyanos

5. Spyware

6. AdWare

7. Ransomware

8. Doxing

9. Phishing

**10. Denegación de servicio
distribuido (DDoS)**

11. Inyección SQL o SQL

12. Whaling o “Caza de Ballenas”



Ataques Cibernéticos



Doxing

Acto de revelar información personal

(Humillar, intimidar, acosar o dañar de otro modo a una víctima).

Siglas claves



Normas IRAN 2791

SGSI (Sistema Gestión Seguridad de la Información).

NIST (National Institute of Standards and Technology).

CSF

Feature	SASE	SSE
Alcance	Redes y seguridad	Security
Components	SWG, CASB, ZTNA, FWaaS, DLP	SWG, CASB, ZTNA
Benefits	Mas Seguro y eficiente forma de conectar usuarios con aplicaciones y datos.	More focused on security
Desventajas	Mas complejo y caro para implementar.	No provee los dispositivos de seguridad que una organización requiere.

SASE -- Security Access Service Edge.

SSE -- Security Service Edge

SGSI -- Sistema de Gestión Seguridad Información

SWG -- Security WEB Gateway.

CASB -- Cloud Access Security Broker.

ZTNA -- Zero "Trust" Network Access

Ataques Cibernéticos



Denegación de:

Servicio

Distribuido (DDoS)



Cracking tools

- ➔ **Aircrack,**
- ➔ **Cain,**
- ➔ **Abel,**
- ➔ **John Ripper,**
- ➔ **Hashcat,**

Los 5 países con la mayor cantidad de cuentas vulneradas fueron:

- **Russia (13.8 million)**
- **France (13 million)**
- **Indonesia (13.2 million)**
- **US (8.4 million)**
- **Spain (3.9 million).**

Ejemplos de Ransomware

Phobos

Sodinokibi

Ryuk

Conti

Pysa

LockBit

Makop

MeduzaLocker

BlackCat



Compañía de Seguridad

Ataques en Latinoamérica

**Ransomware, malware,
troyanos, phishing,
malware móvil y
spyware (SpyLoan}, son
las vulnerabilidades de
México**

Ransomware

**En 12 meses 1.5
millones de ataques**

Brasil	600.000
Ecuador	212.000
México	102.000
Colombia	80.000
Chile	46.000
Argentina	12.000
Panamá	7.900
Costa Rica	5.100
El Salvador	1.600
Guatemala	1.200
Rep. Dominicana	962

5 mayores ciberataques



ILoveYOU - 2000,

Alrededor de 60 millones de equipos son infectados a través de un correo electrónico spam con asunto LoveLetter4YOU. I HATE GOING TO SCHOOL



WANNACRY - 2017,

Ordenadores en toda Europa ven afectados sus sistemas, encriptados sus archivos y bloqueados los accesos de administrador a sus usuarios.



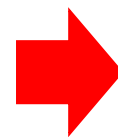
CONFICKER - 2008,

Complejo gusano se infiltra aprovechando una grieta explotable de Windows server, los sistemas vulnerables son Windows 2000, Windows XP, Windows Vista, Windows Server 2003 y Windows server 2008.



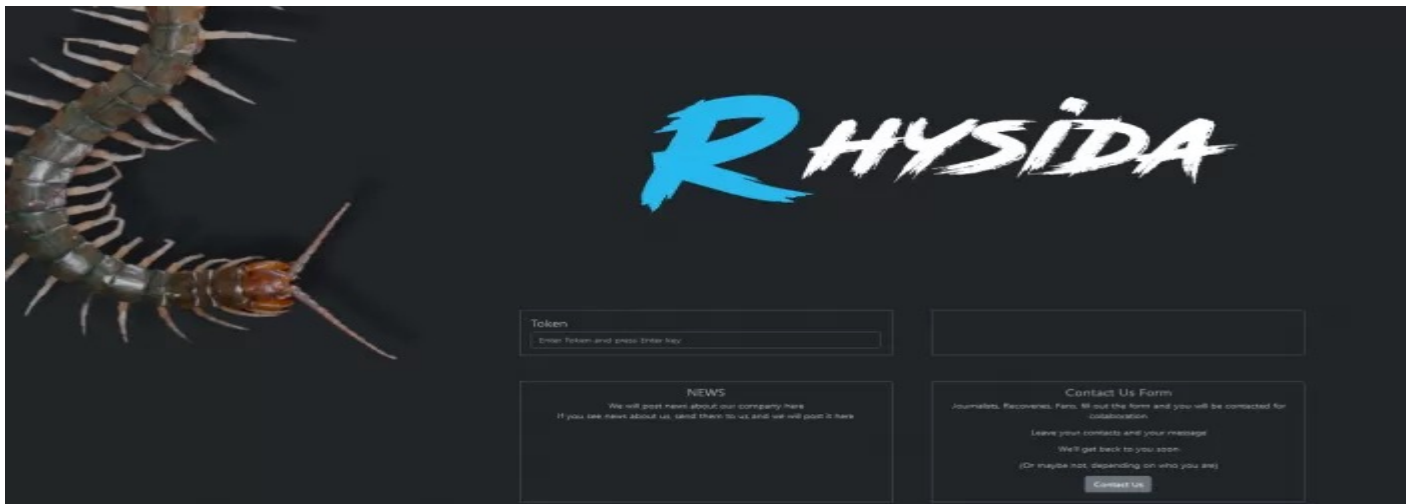
STUXNET 2010,

El espía más sofisticado de nuestros días hace su aparición con un objetivo: Infraestructuras críticas y entornos industriales en Irán, como centrales nucleares o plantas de energía.



PETYA - 2016,

Ransomware que infecta los ordenadores, encripta los datos haciendo imposible su uso para el usuario y pide un rescate a cambio.



¿Qué es y cómo ataca Rhysida?

Este grupo emergió mayo de 2023.

Opera bajo el concepto de Ransomware-as-a-Service (RaaS).

Desde su aparición, centró su atención en América Latina.

Su primer ataque en junio de 2023, en Chile.



WannaCry es el mayor ataque de ransomware de la historia.

Afectó a cientos de miles de sistemas informáticos en todo el mundo.

Causando grandes daños a más de 200.000 ordenadores en

150 países.

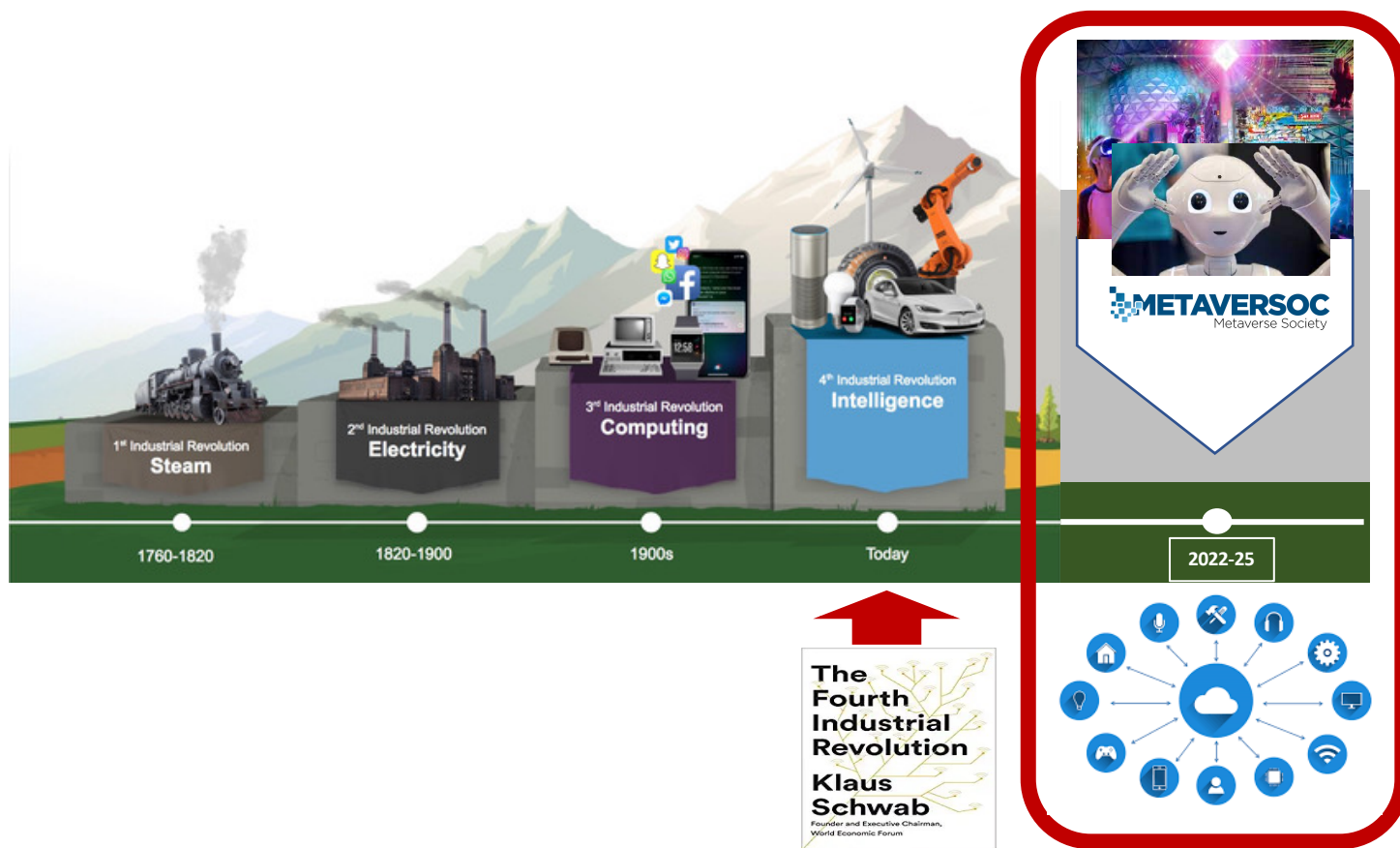
Datos de Interés



.5 % del Mundo es URBE

54% Vivimos en URBE

Industrial Revolutions



¿Qué es Metaverso?

**Es un “Mundo Digital”
donde la gente es
representada por objeto
digitales.**

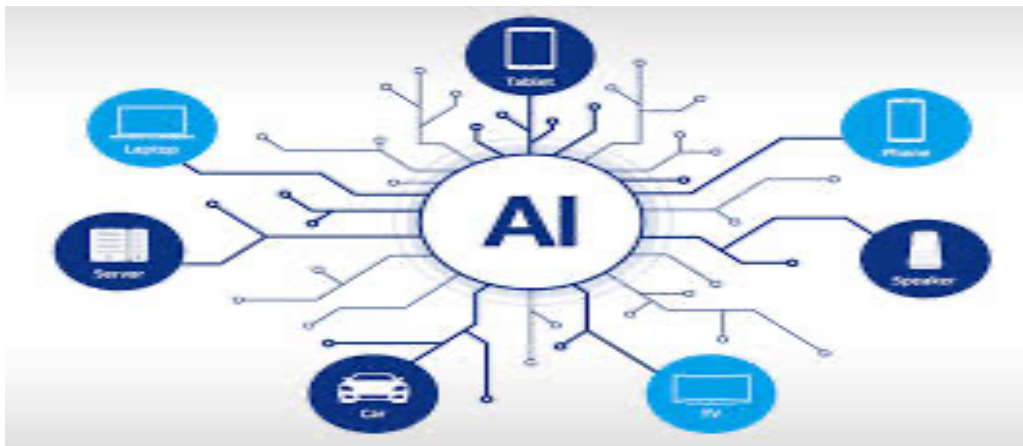
¿Qué es Metaverso?

“Es una **Internet Envevida
donde en lugar de ver
contenido tu estas con el”**

Definición de AI

Muy Simple:

Es la simulación de procesos de inteligencia humana por parte de máquinas o computadora.



Definición de AI

Clásica:

Es la simulación de procesos de inteligencia humana mediante máquinas, especialmente sistemas de cómputo.

Pueden realizar tareas como el aprendizaje, la resolución de problemas, el razonamiento y la toma de decisiones.

Definición de AI

Moderna:

La IA es un campo interdisciplinario que se enfoca en la creación de algoritmos y sistemas capaces de realizar tareas cognitivas que, si fueran realizadas por seres humanos, requerirían inteligencia.

Estas tareas incluyen el procesamiento del lenguaje natural, la visión por computadora, la toma de decisiones, el aprendizaje automático y algo más.

Definición de AI

La Basada en Aprendizaje:

La AI se refiere a la capacidad de una máquina para aprender de la experiencia y mejorar su desempeño en tareas específicas a lo largo del tiempo.

Esto se logra mediante el uso de algoritmos de aprendizaje automático.

Introducción

IA

El sector de defensa se beneficia de su uso.

A medida que se vuelve más popular, el número de aplicaciones no para de crecer.

Es una buena herramienta para tomar la información necesaria para todo tipo de decisiones.

Experiencias más personalizadas.

Reto al cambio.

Que hay que temer a AI

Desplazamiento laboral.

Sesgos y discriminación.

Privacidad, Autonomía y Control.

Impacto en la Economía Global.

Super inteligencia. AGI -



Uso para evitar Ataques a Redes de Información

- ➔ - **Intrusion Detection System.**
IDS
- ➔ - **Malware Analysis.**
MA
- ➔ - **Network Security, Orchestration, Automation and Response.** **SOAR**
- ➔ - **Security Information and Event Management .** **SIEM** . **Security Logs.**
- ➔ - **Machine Learning – Predict and Prevent Network Penetration.** **PPNP**
- ➔ - **Social Media and use of the** **Dark Web.**

IA para prevenir ciberataques

- ➔ **Gestión de contraseñas:** Implementa soluciones de gestión de contraseñas.
- ➔ **Firewalls basados en IA:** Utiliza firewalls basados en IA que puedan adaptarse y aprender de los patrones de tráfico.
- ➔ **Análisis de malware:** Emplea soluciones de análisis de malware basadas en IA para identificar y clasificar automáticamente nuevos tipos de malware.
- ➔ **Respuesta automatizada a incidentes:** Implementa sistemas de respuesta automatizada que puedan tomar medidas rápidas.
- ➔ **Formación y concienciación:** Utiliza la IA para crear programas de formación y concienciación sobre seguridad cibernética personalizados para los empleados.

IA para prevenir ciberataques

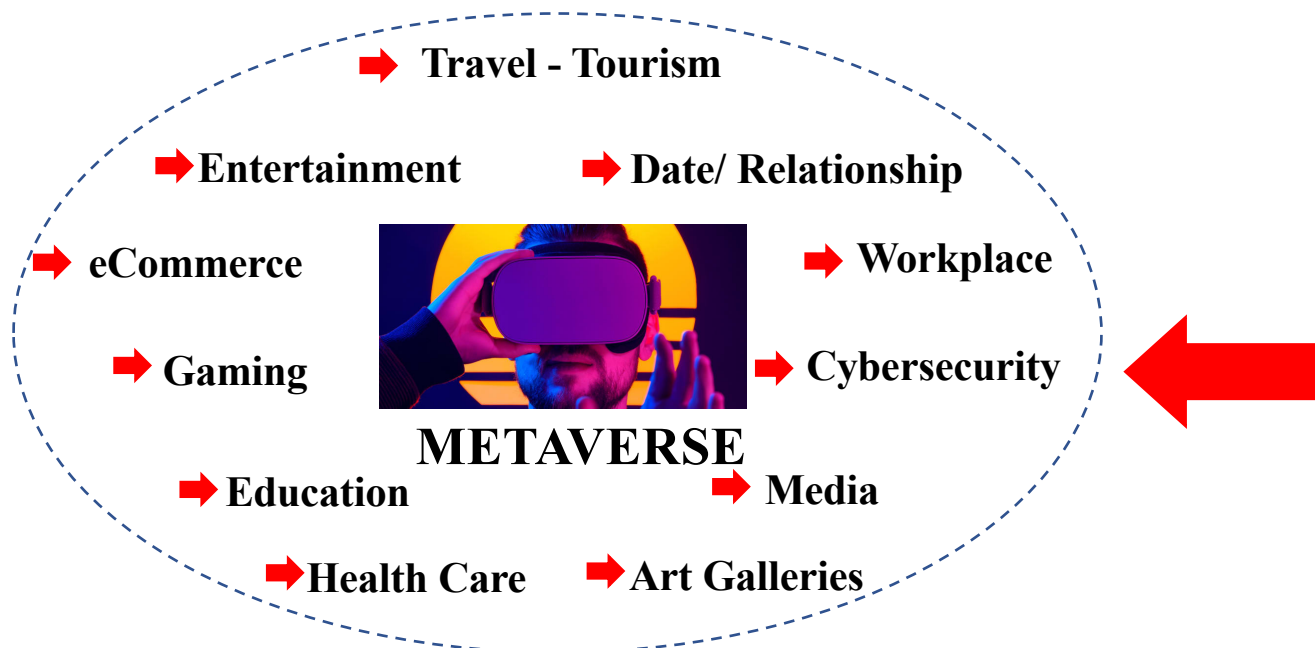
- ➔ **Detección de amenazas y anomalías:** Utiliza algoritmos de aprendizaje
- ➔ **Sistemas de detección de intrusiones (IDS):** Implementa sistemas de detección de intrusiones basados en IA.
- ➔ **Análisis de comportamiento de usuarios:** Utiliza la IA para analizar el comportamiento típico de los usuarios dentro de tu red.
- ➔ **Filtrado de correo electrónico y spam:** Implementa soluciones para evitar phishing y spam.
- ➔ **Análisis de vulnerabilidades:** Utiliza herramientas de escaneo de vulnerabilidades para identificar debilidades en tus sistemas y aplicaciones.

Personal Assistants

- ➔ **Siri**
- ➔ **Alexa**
- ➔ **Watson**
- ➔ **Erica**
- ➔ **Google Assistant**
- ➔ **Cortana**
- ➔ **Irene**
- ➔ **Sherpa**



¿Qué cambiar con AI ?





Mundo Metaverso

METAVERSITY – Open AI – RA/RV Y DAO - Chat GPT - Chatbots



ChatGPT

Tiempo que tardó el mundo en llegar a tener **100 millones** de usuarios:

Telefono: 75 años
iTune: 6.5 años
años Twitter: 4.5 años
Instagram: 2.5 años

Mobile phone: 16 años
Bitcoin, Facebook: 5
Whatsapp: 3.5 años
Apple App Store: 2 años

 **Chat GPT “AI”: Solo 2 Months**

BARD - La competencia de Chat GPT



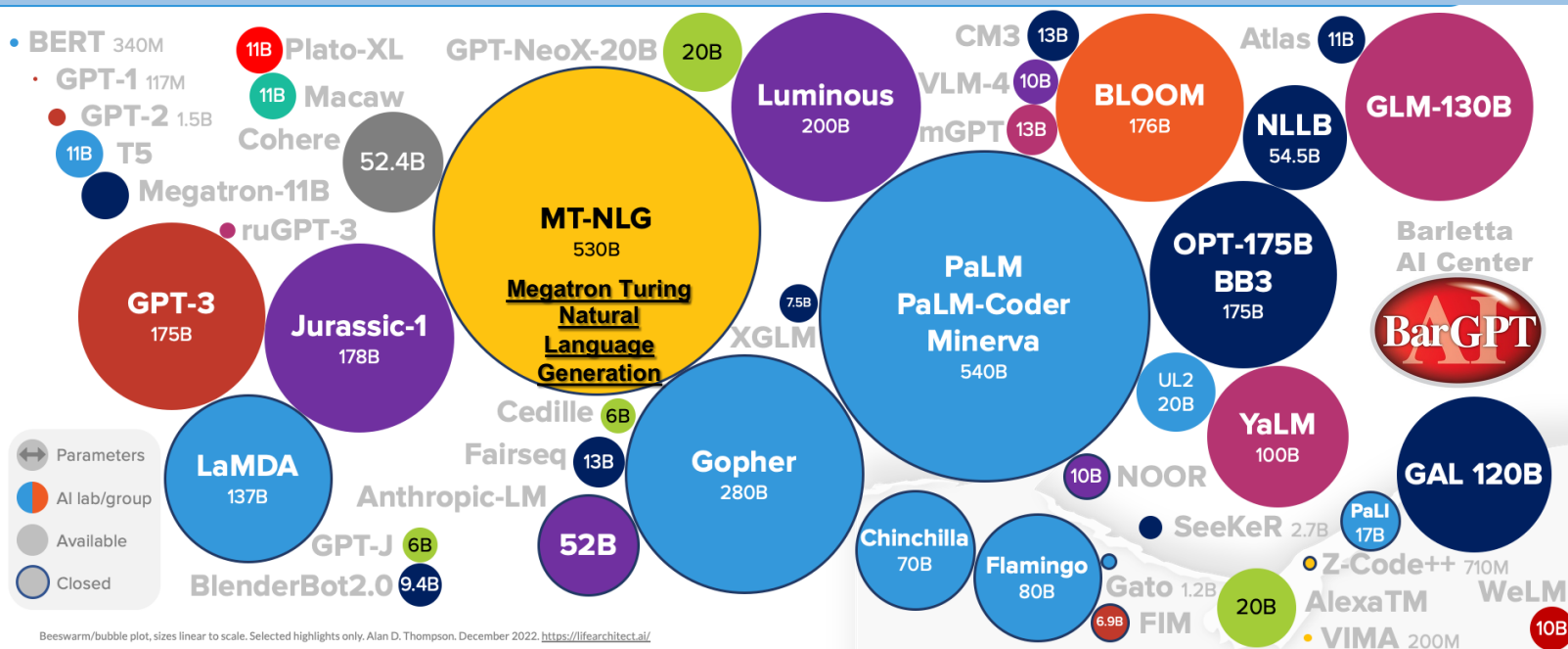
Chatbots

Los **Chatbots** -- IA que interactúan con los humanos. Se basan en:

- ➔ **Procesamiento del Lenguaje Natural (PLN).**
- ➔ **Aprendizaje Automático (AM).**

Analizando lo que se dice o se lee, aprenden cuál es la respuesta a una pregunta concreta.

Language AI Models by size.



LifeArchitect.ai/models

MMLU Benchmark
A good Apology

Bedrock - IA Generativa

Amazon Web Service (AWS)



Tongyi Qianwen ChatGPT de Alibaba



ChatGPT



Está basado en el denominado:

Generative Pre-trained Transformer (GPT)



ChatGPT



Chat GPT 3, pasó pruebas importantes en
USA y si fuera una persona real estaría lista para
ser un buen: **Gerente, Médico o Abogado**

Chat GPT



BarGPT Chatbot
International AI Assistant
Modelo Generativo

P: ¿Quién eres? ¿Vas a cambiar el mundo?

R: Soy **ChatGPT, un modelo de lenguaje de OpenAI.**

No tengo la capacidad de cambiar el mundo, solo brindo respuestas y soluciones basadas en la información con la que fui entrenado.

AGI

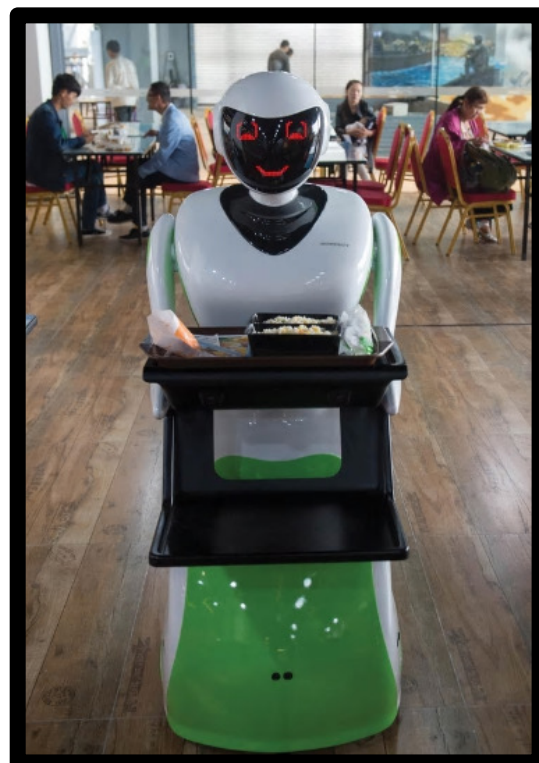
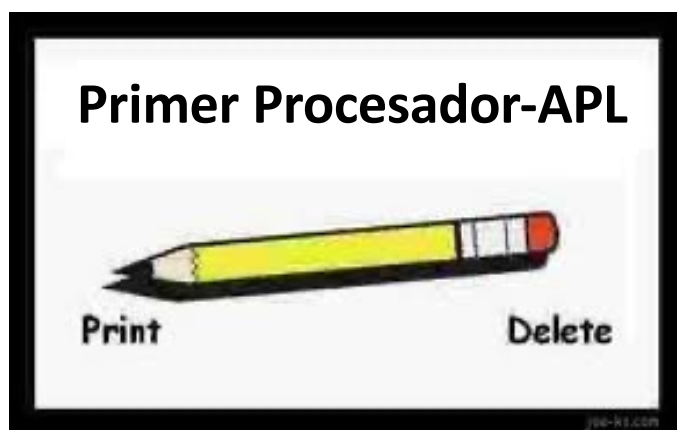
Artificial General Intelligence

- ➔ **AGI** es casi lo mismo que **Inteligencia Humana**
- ➔ **Es la habilidad de las máquinas de pensar y entender como humanos**

DALL·E 2
vs
stable diffusion
vs
Midjourney



Cambios de Paradigmas



Cambios de Paradigmas



Mr. Kaft



Mr. Pepper



GPT 3.5

- Generative Pre-Trained Transformer -

Como accedo al modelo

chat.openai.com



BARD - La competencia de Chat GPT



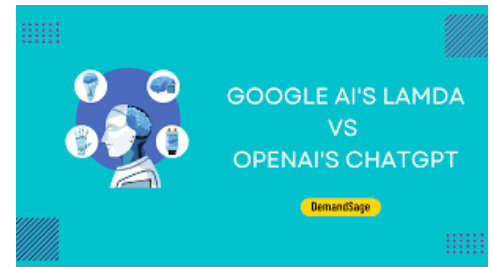
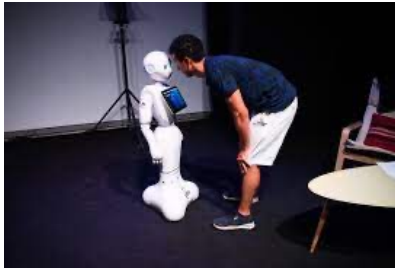
LaMDA



**Lanza su propio ChatGPT:
se llama “**BARD**” y está
basado en LaMDA, su
polémica IA.**

LaMDA

Language Model for Dialogue Applications

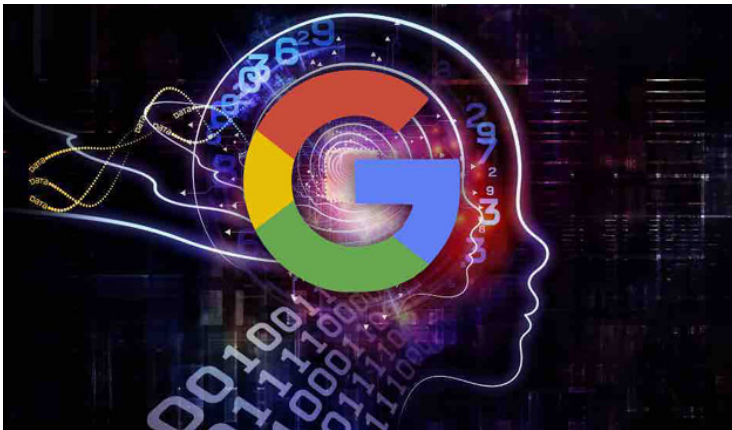


LaMDA

“¿Tiene LaMDA sentimientos?”.

Blake Lemoine, hizo pública la transcripción de una conversación de AI de Google “Modelo de lenguaje para aplicaciones de diálogo”.

LaMDA



ChatGPT



Está basado en el denominado:

Generative Pre-trained Transformer (GPT)



ChatGPT



Chat GPT 3, pasó pruebas importantes en
USA y si fuera una persona real estaría lista para
ser un buen: **Gerente, Médico o Abogado**

ChatGPT



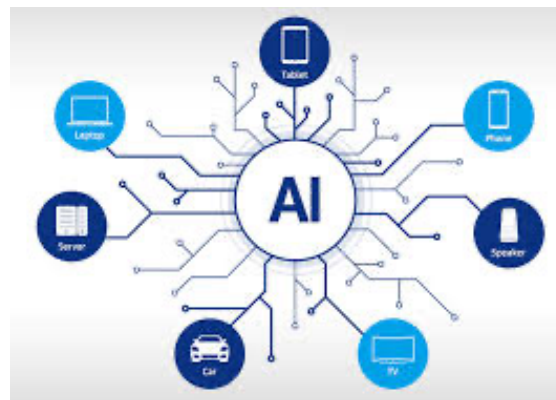
P: ¿Quién eres? ¿Vas a cambiar el mundo?

BarGPT Chatbot
International AI Assistant
Modelo Generativo

R: Soy **ChatGPT, un modelo de lenguaje de OpenAI.**

No tengo la capacidad de cambiar el mundo, solo brindo respuestas y soluciones basadas en la información con la que fui entrenado.

Herramientas AI



Enfrentando el Futuro

Innovación



● **Hacer
cosas un
poco mejor**

Disrupción



● **Hacer
nuevas
cosas**

● **Hacer
cosas que
dejan
obsoletas
las
anteriores**

Disrupción

Es la interrupción de operaciones normativas para hacer algo nuevo, atractivo, eficiente y motivador.

La innovación Disruptiva

Crear productos simples **impacten** y se conviertan en líderes en el mercado.

¿Cómo? • Mejorando la tecnología ya existente para hacer **cambios radicales.**

Julia White – CEO Microsoft



The Perfect Hologram

Julia White en las Vegas

Muchas Gracias



www.miamioportunidad.com



barletta@barnews.com



+ 1 305-803-2226



