



La ciberseguridad y los analíticos en tiempos de la IA

República Dominicana | Octubre 2023



Luis Bustamante

Business Information Security
Officer LATAM at Equifax



Líder global en datos, analítica y tecnología.

Equifax juega un rol esencial en la economía al ayudar a compañías de diversas industrias como la automotriz, comunicaciones, servicios, servicios financieros, fintech, salud, seguros, hipotecas, comercio y gobierno a tomar **decisiones estratégicas de negocio con mayor confianza.**



Operamos en
24 países



NYSE: EFX
Ingreso en 2022:
US\$5,1 mil millones



+14 mil empleados
en el mundo

Ayudamos a las personas a alcanzar su mejor potencial financiero



Tenemos una marca sólida - **122 años de historia y presencia en 24 países.**



Somos líder global en nuestro rubro de negocio.



Garantizamos legalidad y transparencia.



Data
Información actualizada y confiables



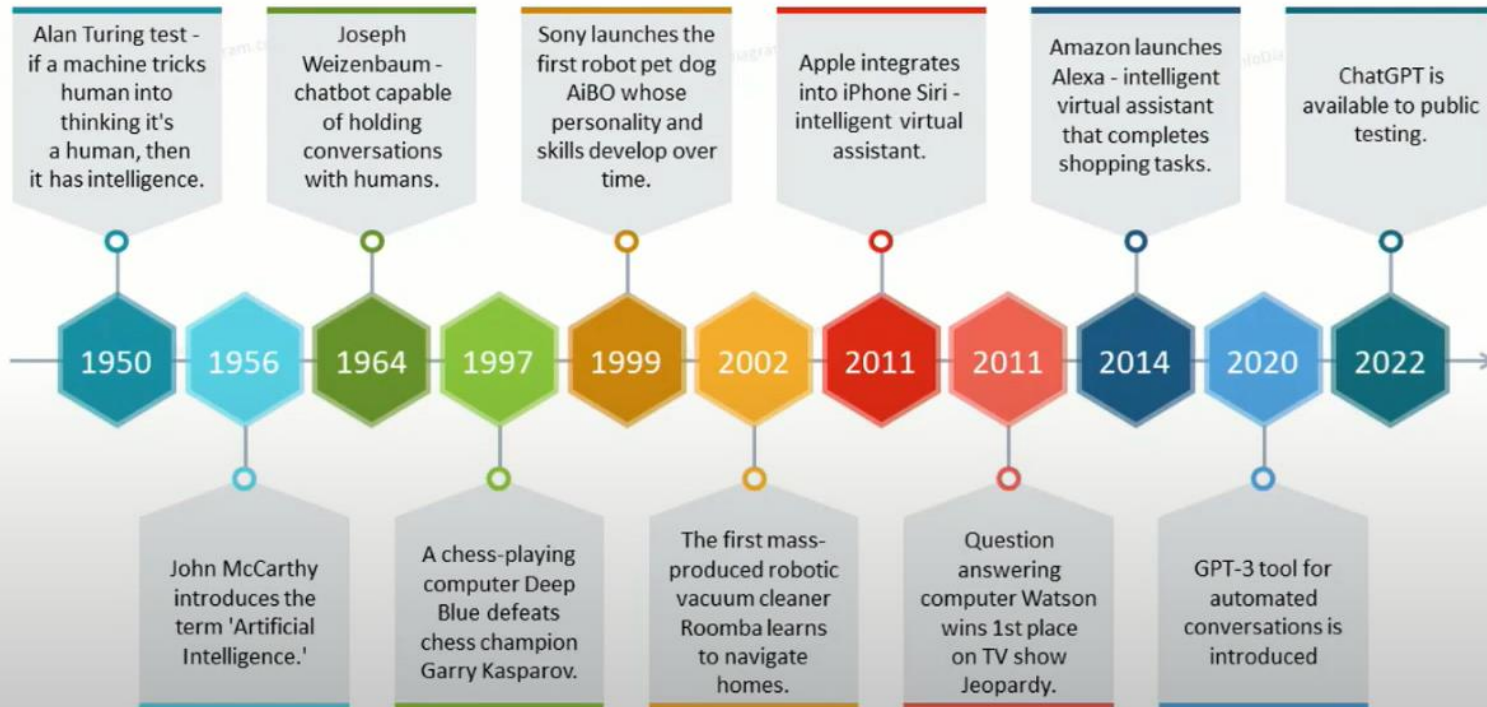
Analíticos
Diversas fuentes de información. Visión del individuo.



Tecnología
Plataforma de BIG DATA que permite el rápido procesamiento de información.



Y ahora tenemos IA...



Algunos aspectos importantes de la IA



Aprendizaje Automático

Uso de datos de muestra para entrenar programas informáticos para reconocer patrones basados en algoritmos.



Redes Neuronales

Sistemas informáticos diseñados para imitar las neuronas del cerebro.



Uso general de la IA

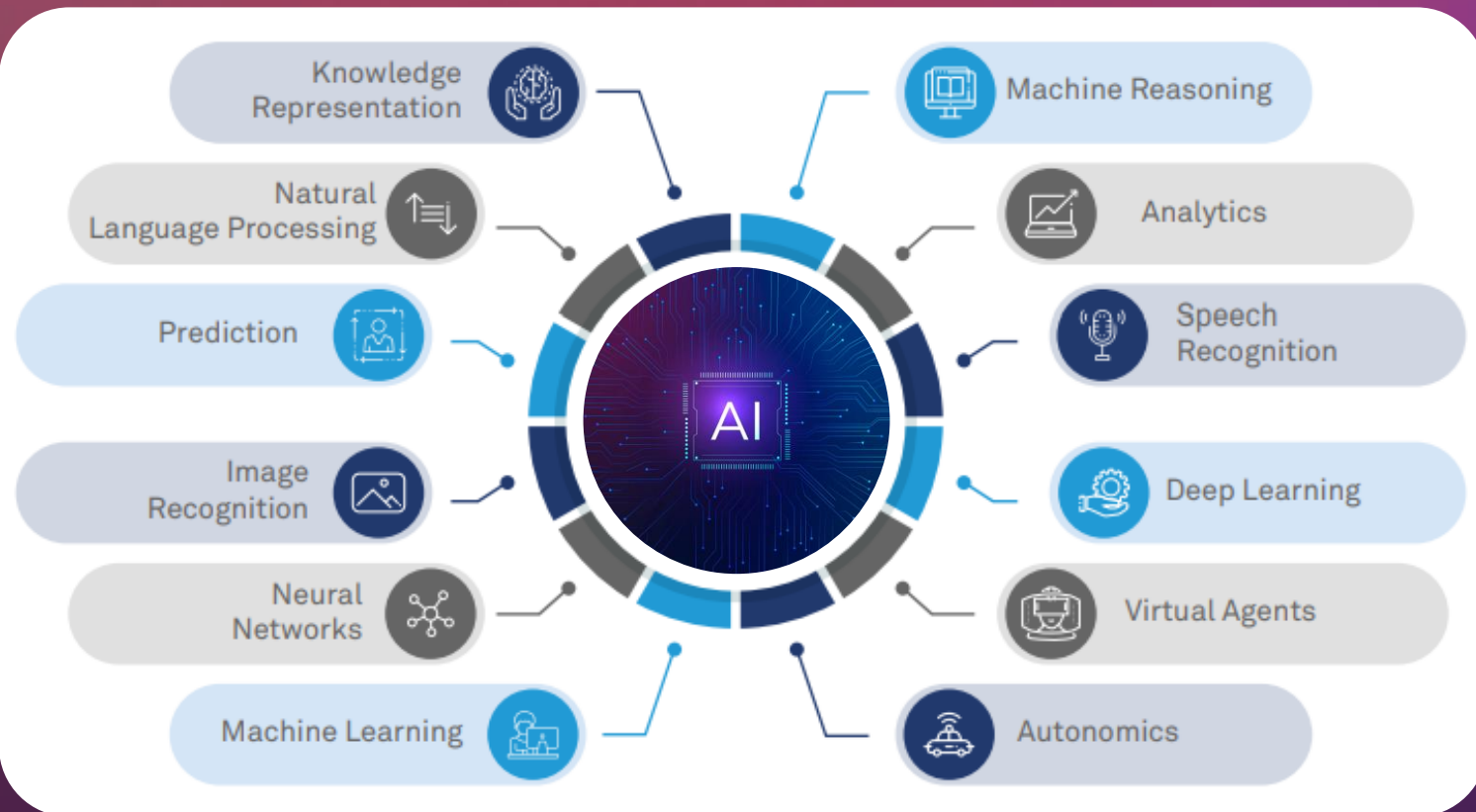
Máquinas que pueden ayudar a las personas sin participación humana real.



Interpretación de lenguaje natural humano

La capacidad de comprender el habla, así como comprender y analizar documentos.

Funciones que podemos tener en la IA



En Equifax ya usamos estas capacidades.

Kount permite a los usuarios tomar decisiones rápidas y precisas a gran escala mediante la **simulación en tiempo real** del proceso de decisión de los analistas de fraude más experimentados.



[illegible]

Riesgos generales de la IA

Vectores de Amenazas

Error humano, Ingeniería Social
Compromiso

Fallas en los sistemas,
Vulnerabilidades, Errores en
los procesos

Ataques milimétricos a los
Queries y respuestas de los
boots

Puntos de entrada
débiles/Maliciosos

Tipos de Daños

Robo de datos, Dinero,
Propiedad intelectual

Activos (Humanos, físicos,
de sistemas) daños de
manipulación

Manipulación de modelos
(Alteración de reglas de
negocio)

Datos falsos y exposición
indebida

Medidas Para Gestionar el Riesgo

Integridad
enfoque humano,
responsabilidad y concientización

Segmentación de redes,
aseguramiento de los endpoints,
gestión de accesos con validación
de la autenticidad

OPs Model, un modelo de
integridad de la IA, check points.

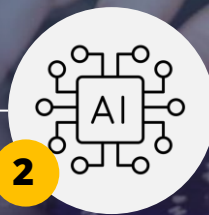
Protección de la infraestructura
mediante detección y
aislamiento de ambientes
infectados

TOP 5 de Investigaciones necesarias para IA y CyberSecurity

**1**

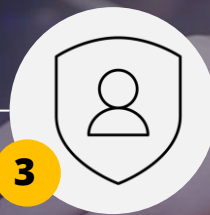
Bancos de Test

Generar bancos de Test (Bases de Conocimiento) para estudiar y optimizar el rendimiento de herramientas y tecnologías basadas en ML utilizadas para la ciberseguridad.

**2**

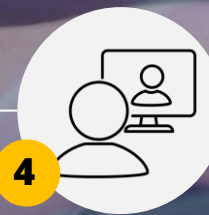
Desarrollo de herramientas de test

Desarrollo de herramientas de test de penetración basadas en IA y ML para encontrar y explotar vulnerabilidades de seguridad para evaluar el comportamiento de los atacantes.

**3**

Marcos estandarizados

Desarrollo de marcos estandarizados que evalúen la preservación de la privacidad y la confidencialidad de los flujos de información, así como el sistema diseñado.

**4**

Modelos de entrenamiento de IA

Desarrollo de modelos de entrenamiento de IA para profesionales que utilizan escenarios del mundo real.

**5**

Observatorio de la IA

Establecer un observatorio de la IA y las amenazas a la ciberseguridad que vienen a través del uso de ésta.

Medidas para enfrentar las amenazas de la IA

Monitorización Post Producción

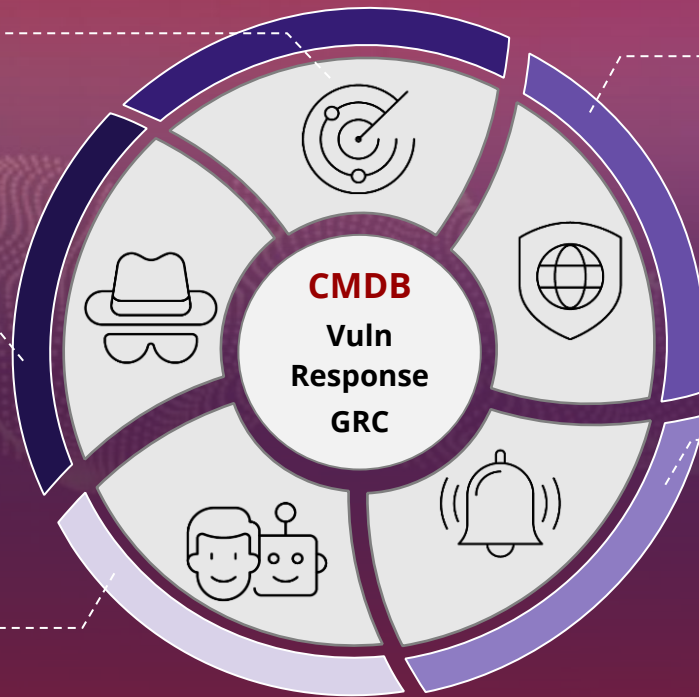
- Revisión periódica de métricas de indicadores.
- Controles de identificación temprana de anomalías en el desempeño de modelos.

Supervisión de la Implementación

- Pruebas suficientes de los Modelos
- Indicadores
- Pruebas de Penetración
- DAST & SAST

Revisión Temprana de Modelos de IA

- Validación de resultados esperados
- Pruebas de Datos



Monitorización continua de los Riesgos

- Análisis de Riesgos optimizado y maduro enfocado en los modelos según su complejidad.

Supervisión de la Arquitectura de Datos y de la Infraestructura

- Actividades Definidas para Gestion de Datos y protection de modelos sobre todo aquellos que manipulan datos de comportamiento.

Recomendaciones generales de seguridad.



Evaluar los riesgos de seguridad usando modelos de amenazas/marcos de referencia conocidos.



Utilizar prácticas de codificación segura y modelos de desarrollo seguro.



Modelos de datos optimizados para gestionar datos generados, recolectados y gestionados por los modelos de IA.



Documentar los modelos de manera clara, que permita las auditorías de los mismos con validación de pruebas de resultados.



¡Muchas gracias!

República Dominicana | Octubre 2023

