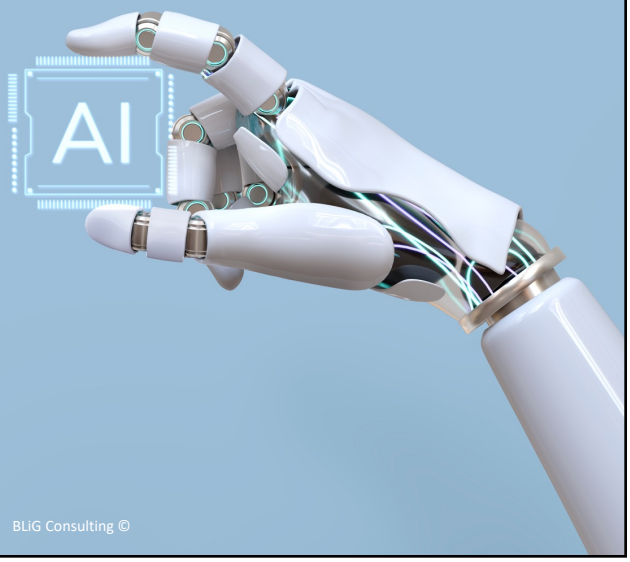
Ciberseguridad en la Era de la Inteligencia Artificial: Desafíos y Oportunidades

Dr. Gilberto Crespo
Cyber & Technology SME | Professor
BLiG Consulting
Octubre 29, 2023

1

Agenda

- Definiciones
- Triada de Ciberseguridad
- Tecnologías Emergentes
- Estadísticas
- Desafíos y Cómo Protegernos
- Q&A



2

Definiciones

- **Ciberseguridad:** *Prevención de daño a, protección de, y restauración de computadoras, sistemas y servicios de comunicaciones electrónicas (wifi) y cable (cobre, figura), incluida la información contenida en los mismos, para asegurar su *disponibilidad*, *integridad*, *autenticación*, *confidencialidad* y *no-repudio*.
- **Inteligencia Artificial (IA):** *La capacidad de un dispositivo para realizar *funciones que normalmente se asocian con la inteligencia humana, como:*
  - Ei.: razonamiento, aprendizaje y auto-mejora, reconocimiento de voz, la toma de decisiones y la traducción entre idiomas, entre muchas otras.

**Fuente: National Institute of Standards and Technology (NIST, Oct. 2023)*

BLiG Consulting ©

3

La Triada de Ciberseguridad

Confidencialidad
Garantizar que la información sea accesible sólo para aquellos autorizados a tener acceso.

Integridad
Velar por la exactitud y exhaustividad de la información y de los métodos de tratamiento.

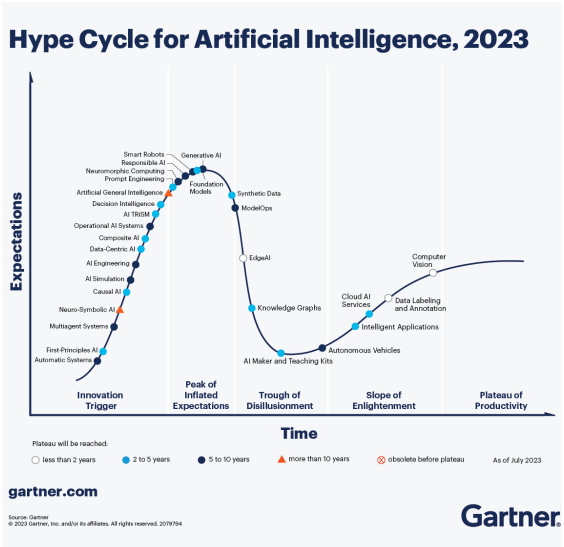
Disponibilidad
Garantizar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea necesario.

BLiG Consulting ©

4

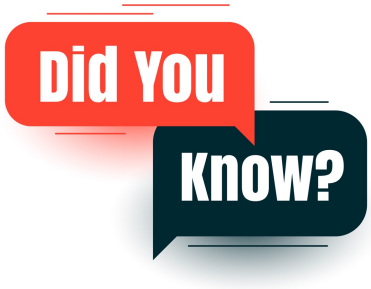
Tecnologías Emergentes

5



6

Contexto Actual

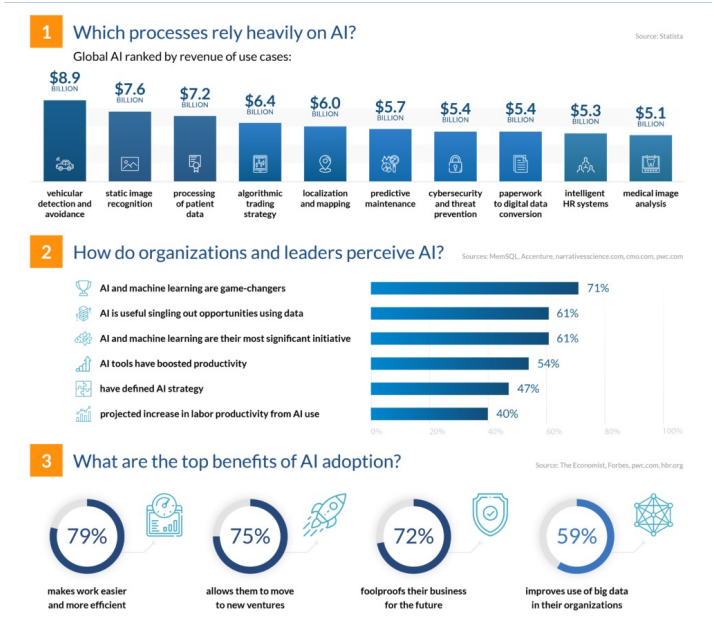


- Actualmente, **el 85%** de las empresas ***están implementando o planean implementar*** soluciones de IA en sus operaciones.
  - La IA puede proporcionar una ventaja competitiva significativa a las empresas al ***automatizar tareas y procesos***, ***mejorar la eficiencia y la precisión***, y ayudar en la ***toma de decisiones***.
- Sin embargo, el uso de la IA también puede presentar riesgos de seguridad significativos.
  - **60%** de las empresas que han implementado soluciones de IA han reportado ***preocupaciones de seguridad*** en los últimos 12 meses. Estos riesgos incluyen, pero no se limitan a:
    - la ***exposición de datos*** sensibles, la ***manipulación de algoritmos*** y la creación de ***puertas traseras para ciberataque***s.

BLiG Consulting ©

7

Estadísticas Clave de IA que Debes Conocer



BLiG Consulting ©

8

Desafíos de la IA

- Ataques Avanzados
- Falsificación de Contenido
- Escasez de Expertos

9

Estadísticas Clave de Ciberseguridad en la Adopción de IA

Tema	Estadística	Fuente
Ataques Deepfake	Se espera que aumente un 250% para 2023	Forrester
Automatización en Ciberdefensa	El 45% de las empresas utilizan soluciones de IA para la ciberseguridad	IBM
Adopción de la IA en las plataformas de seguridad	Más del 50% de todas las nuevas plataformas de seguridad empresarial utilizarán el aprendizaje automático para 2025	Gartner
Tamaño del mercado de la IA en ciberseguridad	Se espera que alcance los 38,200 millones de dólares en 2026	Markets&Markets
Vulnerabilidades en los modelos de IA	El 98% de las empresas que implementan modelos de IA carecen de medidas de seguridad suficientes	Universidad de Cambridge

10

Desafíos Principales con la IA y Cómo Protegernos

Amenaza	Descripción	Protección
Manipulación de Datos	Atacantes introducen datos erróneos durante el entrenamiento de la IA, sesgando sus decisiones.	Uso de datos de entrenamiento verificados y supervisión constante de las fuentes de datos.
Ataques Adversarios	Atacantes introducen entradas diseñadas para confundir a la IA, haciendo que tome decisiones incorrectas.	Implementar sistemas de detección de anomalías y entrenar la IA con ejemplos de estos ataques.
Falta de Explicabilidad	Modelos de IA que no pueden explicar sus decisiones pueden resultar en acciones no deseadas.	Usar modelos de IA más transparentes o herramientas de interpretación.
Uso Malintencionado de la IA	La IA se utiliza para actividades maliciosas, como deepfakes o ciberataques automatizados.	Establecer regulaciones y controles estrictos sobre el uso y acceso a herramientas de IA avanzadas.
Dependencia Excesiva de la IA	Confiar demasiado en la IA sin supervisión humana puede llevar a errores no detectados.	Mantener una supervisión humana activa y establecer puntos de control donde las decisiones sean revisadas.
Desconocimiento y/o Desinformación	Fortalecer la educación, capacitación y adiestramiento.	Mejorar la formación en ciberseguridad y fomentar una comprensión más profunda de la IA.

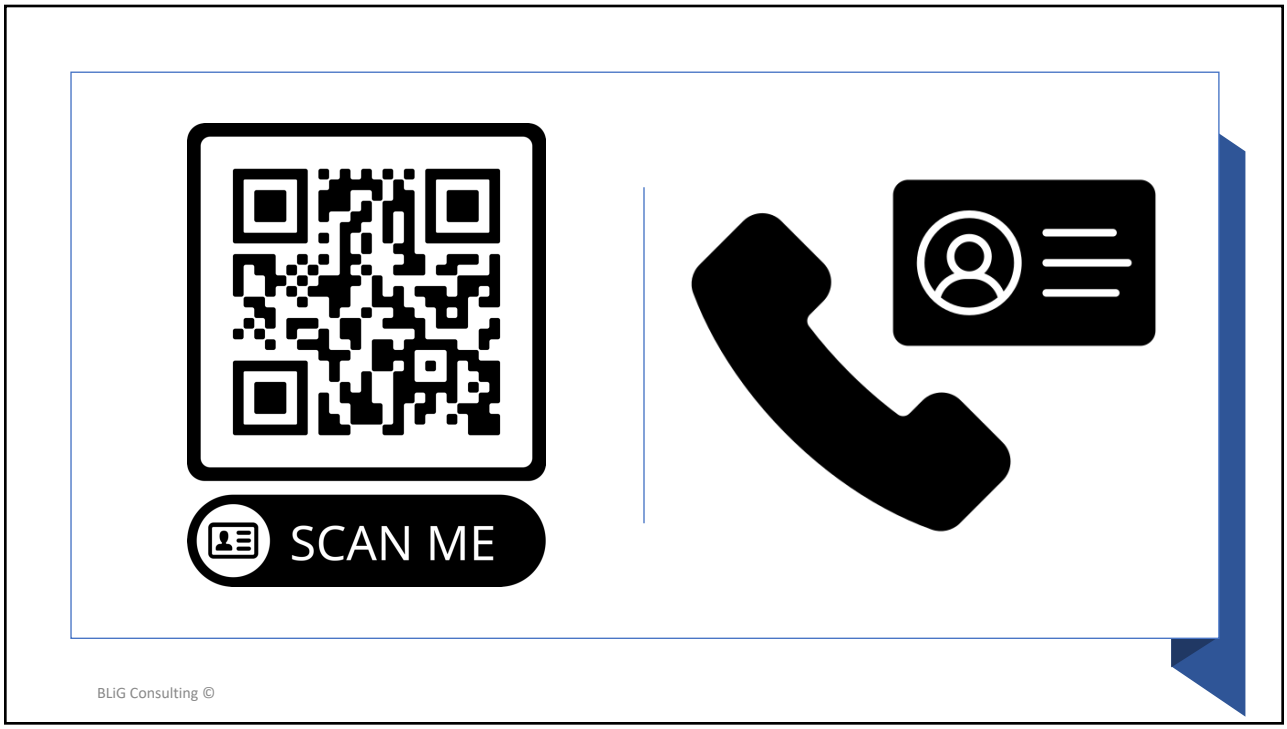
11

12

Pre-Post Prueba

- La Inteligencia Artificial no tiene vulnerabilidades específicas; los desafíos de ciberseguridad para la IA son los mismos que para cualquier otro software.
- La manipulación de datos o "data poisoning" puede ser utilizada para alterar las decisiones tomadas por sistemas basados en Inteligencia Artificial.
- Todas las regulaciones de protección de datos, como el GDPR, excluyen a los sistemas basados en Inteligencia Artificial debido a su naturaleza avanzada.
- Una tendencia emergente en ciberseguridad es la utilización de Inteligencia Artificial para predecir y prevenir ataques antes de que ocurran.
- El reconocimiento facial, una aplicación popular de la Inteligencia Artificial, es completamente infalible y no puede ser engañado o manipulado.

13



14