Índice

Fundamentos de la inteligencia artificial

La inteligencia artificial es una rama de la informática que busca crear sistemas y máquinas capaces de realizar tareas que tradicionalmente requieren inteligencia humana, como aprender, razonar, resolver problemas y tomar decisiones. Incluso de crear máquinas creativas.

En la actualidad los algoritmos desarrollados en IA son muy eficientes, tanto que les permite a las máquinas aprender y dar respuesta a escenarios diferentes, incluso en aquellos escenarios para los que no fueron creadas.

Tipos de inteligencia artificial

Inteligencia Artificial Estrecha (ANI): También conocida como IA débil o limitada, es el tipo más común en uso actualmente. Diseñada para tareas específicas y limitadas, carece de conciencia y emociones. Ejemplos: asistentes virtuales como Siri o Alexa, sistemas de reconocimiento de voz

IA Generativa: subcategoría de ANI, que crea contenido nuevo a partir de datos existentes. Ejemplos: GPT-4 para generar texto, DALL-E para crear imágenes, etc.

Inteligencia Artificial General (AGI), también llamada IA fuerte o generalizada: capacidades cognitivas similares a las humanas, que puede realizar múltiples tareas y aprender autónomamente. Entre sus características están el aprendizaje y adaptación a diferentes situaciones, la flexibilidad cognitiva, ***la autoconciencia y metacognición***, y la creatividad y ***comprensión*** de emociones.

Superinteligencia Artificial (ASI): representa el nivel más avanzado y **teórico** de IA. Supera la inteligencia humana en todos los aspectos, como capacidad de procesamiento extremadamente alta, aprendizaje acelerado, auto mejora continua y generalización de conocimiento en múltiples dominios

---

Conceptos ligados a los tipos de IA

1) Máquinas Reactivas: las máquinas reactivas son el tipo más simple y antiguo de inteligencia artificial. Estas máquinas interactúan con el entorno, pero no mantienen una representación interna del mismo. No tienen memoria, por lo que no pueden aprender de interacciones pasadas ni mejorar su rendimiento. Toman decisiones inmediatas basadas únicamente en la información disponible en el momento presente, realizando acciones específicas reaccionando a estímulos determinados y no pueden ejecutar tareas que requieran adaptación o entendimiento del contexto.

Un ejemplo famoso de máquina reactiva es Deep Blue, la supercomputadora de ajedrez creada por IBM que derrotó al campeón mundial Garry Kasparov en 1997. Otra máquina de este tipo podría ser un robot basado en Arduino que esquiva obstáculos.

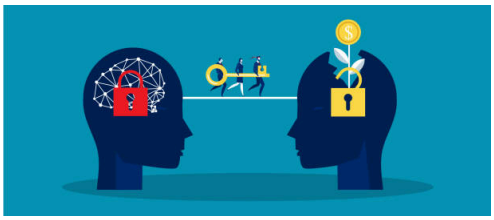
2) Máquinas con Memoria Limitada: las máquinas con memoria limitada son un paso adelante respecto a las máquinas reactivas. Sus características principales incluyen:

1. Tienen una pequeña cantidad de memoria disponible.
2. Pueden aprender de los datos y crear pequeñas bases de datos a partir de su historial de interacciones
3. Son capaces de tomar decisiones basadas en experiencias recientes, aunque de manera limitada
4. Pueden generar aprendizajes a partir del contenido al que son expuestas.

Ejemplos de aplicaciones de máquinas con memoria limitada incluyen sistemas de reconocimiento facial (que almacena información de las caras escaneadas y puede usarla para

identificar caras nuevas) , asistentes virtuales y chatbots básicos. En general, clasificadores bayesianos y redes neuronales sin memoria a largo plazo.

3) La teoría de la mente (ToM): es la capacidad cognitiva que permite a una persona comprender y predecir el comportamiento, pensamientos, creencias, deseos e intenciones de otros individuos y de sí mismo.



Esta habilidad implica atribuir estados mentales a uno mismo y a los demás (estoy-está enfadado, alegre, nervioso, etc.) , reconocer que otras personas pueden tener puntos de vista, creencias y deseos diferentes a los propios e inferir y predecir el comportamiento ajeno basándose en la comprensión de sus estados mentales (aquella persona está triste; es posible que se vaya a casa y abandone la fiesta).
La ToM se desarrolla típicamente entre los 3 y 4 años de edad, a través de interacciones sociales y relaciones interpersonales. Es fundamental para la interacción social efectiva, permitiendo interpretar el lenguaje no literal, como la ironía y las metáforas, desarrollar empatía y comprender estados emocionales ajenos y detectar creencias falsas en otros.

Esta capacidad es crucial para navegar el mundo social y se considera un aspecto clave de la cognición social. Su desarrollo adecuado contribuye significativamente a la habilidad de una persona para interactuar eficazmente en diversos contextos sociales.

En el contexto de la IA, ***la ToM implica que un sistema o máquina sea capaz de comprender y modelar los estados mentales de los seres humanos, pudiendo así interactuar de manera efectiva con ellos***. Aún en desarrollo y evolución, se utiliza en asistentes virtuales, chatbots o agentes de negociación, que pueden entender las intenciones de la otra parte y llegar a acuerdos favorables con otros.

4) Autoconciencia. Es un concepto , por ahora, teórico y complejo. Consistiría en que la máquina adquiriese una de las más altas características humanas, la capacidad de reconocer la propia existencia y la comprensión de sí mismo. Si una máquina lo consiguiera, sería capaz de sentir emociones, pensar en las consecuencias de sus acciones, tener experiencias subjetivas y desarrollar una identidad, reflexionando sobre sí misma.

Por ahora es una cuestión hipotética, planteada a largo plazo, aunque se trabaja en ella. Ninguna IA ha demostrado tener autoconciencia (ver ejemplo). Las líneas de investigación se centran en desarrollar redes neuronales y algoritmos que simulan la actividad cerebral humana, y sistemas que sean capaces de reconocer sus propios errores y solucionarlos.

Lograr la autoconciencia en la IA plantearía profundos debates filosóficos, científicos y éticos. Una máquina autoconsciente podría pensar por sí misma y tomar decisiones sin la ayuda de un ser humano.

Impacto social de la inteligencia artificial

La inteligencia artificial (IA) ha tenido numerosos impactos positivos en diversos ámbitos:

1.- Personas con Discapacidad, mejorando su calidad de vida.

- Sistemas de reconocimiento de voz y texto-a-voz permiten una mejor comunicación.
- Prótesis inteligentes y dispositivos de asistencia adaptables.
- Aplicaciones de navegación para personas con discapacidad visual.

2.- Creaciones Artísticas, generando nuevas formas de expresión y nuevas formas de arte únicas (usando algoritmos de aprendizaje profundo). Los artistas también se benefician de herramientas de IA que potencian su creatividad.

3.- Productividad y Calidad, automatizando tareas repetitivas y liberando tiempo para actividades creativas. Reduciendo significativamente los errores humanos, mejorando la calidad del producto final y optimizando procesos de producción y líneas de montaje.

4.- Búsquedas y Procesamiento de Información, permitiendo motores de búsquedas más precios y personalizados, y el análisis de grandes volúmenes de datos en tiempos record.

5. - Otros Impactos Positivos / aplicaciones.

- **Salud**: Diagnósticos más precisos y precoces, y desarrollo de tratamientos personalizados.
- **Agricultura**: Optimización de cultivos y predicciones meteorológicas más precisas.
- **Finanzas**: Detección de fraudes y asesoramiento financiero personalizado.
- **Comercio**: pronósticos de venta.
- **Transporte**: Optimización de rutas y reducción de accidentes de tráfico. Localización de vehículos. Coches autónomos. Relación con el concepto de *smart city*.
- **Atención al cliente:** Chatbots disponibles 24/7 para resolver consultas.
- **Asistentes personales virtuales:** nos ayudan a automatizar procesos en casa (domótica) o en nuestros móviles, mediante comandos de voz. Tenemos a Alexa, Siri o Cortana.
- **Asistentes de voz para empresas:** chatbots que interactúan con los usuarios (por voz o por texto) y llevan a cabo operaciones de consulta o comerciales sin necesidad de personas físicas.
- **Reconocimiento facial:** detecta a personas parametrizando sus caras, lo cual ayuda a la policía a encontrar delincuentes. También puede servir como medio de seguridad en móviles y dispositivos.
- **Selección de contenidos en redes sociales**, permitiendo la personalización.

Pero también tiene una cara negativa:

1. Uso fraudulento de datos personales, por filtraciones o fallos de seguridad.
2. Falsificaciones de fotos o vídeos, suplantando la personalidad de alguien con malas intenciones.
3. Transformación de empleos y riesgo de pérdida de puestos de trabajo.
4. Modificaciones en el comportamiento de los seres humanos. Por ejemplo, niños que tratan a seres humanos como lo hacen con máquinas y robots.
5. Errores de la inteligencia artificial, que pueden acarrear problemas (por ejemplo, un reconocimiento facial erróneo puede llegar a multar a la persona equivocada). Entre los errores de las IAs, los más importantes están relacionados con el concepto de **sesgo**.

Un sesgo se refiere a errores sistemáticos en los algoritmos o modelos de machine learning que producen resultados injustos, discriminatorios o que favorecen a ciertos grupos sobre otros.

Estos sesgos pueden manifestarse de diversas formas:

1. **Discriminación**: Los sistemas de IA pueden generar resultados que discriminan por raza, género, edad u otras características.
2. **Perpetuación de estereotipos:** La IA puede reforzar y propagar estereotipos sociales y culturales existentes.
3. **Falta de equidad:** Los sesgos pueden llevar a decisiones injustas en áreas como educación, empleo y justicia..
4. **Errores sistemáticos:** Los sesgos causan errores repetitivos y predecibles en los resultados de la IA

Los sesgos en la IA pueden originarse de diversas fuentes: diseño de algoritmos incorporando prejuicios, equipos de desarrolladores con falta de diversidad, etc. Pero normalmente encontramos sesgos en la IA cuando ésta necesita ser entrenada a base de datos, y estos modelos de datos son sesgados, es decir, no tienen en cuenta todas las posibilidades.

El caso que denunció Joy Buolamwini es especialmente significativo. Esta activista e informática fundó la Algorithmic Justice League, una organización que buscaba desafiar el sesgo del software en la toma de decisiones. Desarrollando su trabajo de investigación en el MIT Media Lab averiguó que los sistemas de reconocimiento facial no reconocían correctamente las caras de las mujeres de piel oscura al haber sido entrenados mayoritariamente con datos de personas de piel clara.

Un sistema que tomara decisiones, por ejemplo, para contratar personal para una empresa en función de datos faciales podría estar sesgada, favoreciendo un grupo étnico en detrimento de otro.

Como usamos cada vez más la IA en los procesos de toma de decisiones, tenemos que asegurarnos que no está influenciada por sesgos, intencionales o no.

Big data

Big Data es un concepto que describe ***enormes volúmenes de datos*** que son tan grandes y complejos que superan la capacidad de procesamiento de las herramientas tradicionales.

Hoy en día la generación y análisis de grandes cantidades de datos es crucial en múltiples campos: salud, industria, marketing, investigación científica , logística, seguridad…

Las siete V del Big Data son atributos que caracterizan y definen los aspectos fundamentales de los grandes volúmenes de datos:

1. **Volumen**: se refiere a la enorme cantidad de datos generados y almacenados. Pueden provenir de muchas fuentes: redes sociales, dispositivos IoT (sensores), transacciones comerciales, registros de actividad, etc.
2. **Velocidad**: describe el ritmo rápido y constante al que se generan, procesan y analizan los datos. Es deseable que se interpreten en tiempo real o con una latencia (retraso) bajo.
3. **Variedad**: indica la diversidad de tipos y fuentes de datos, que pueden ser estructurados (formato predefinido y estandarizado), no estructurados o semiestructurados. Los datos pueden recopilarse de diversos formatos, como textos, imágenes, vídeos o audios.
4. **Veracidad**: Se relaciona con la calidad, fiabilidad y precisión de los datos recopilados. A menudo las bases de datos son incompletas o inexactas, lo que hace que sean poco fiables. Pensemos que pueden provenir de múltiples fuentes y que el volumen de datos es muy grande. Existen mecanismos y procesos para evaluar y garantizar su veracidad.
5. **Valor**: Representa la capacidad de extraer información útil y beneficiosa de los datos para la toma de decisiones. En definitiva es el fin último de las bases de datos, extraer conocimiento de ellas. Este conocimiento permite a las empresas y organismos que manejan las bases de datos descubrir oportunidades y crear valor añadido.
6. **Visualización**: Se refiere a la presentación clara y comprensible de los datos procesados. Comúnmente de forma gráfica permite comprenderlos, identificar patrones y comunicar información de forma clara y precisa.
7. **Viabilidad**: Describe la capacidad de una organización para gestionar y utilizar eficazmente los grandes volúmenes de datos con las herramientas de las que dispone. Incluye infraestructura de almacenamiento, técnicas de procesamiento, algoritmos de análisis y capacidad de cómputo.

Bases de datos distribuidas

Una base de datos distribuida (**BDD**) es un conjunto de múltiples bases de datos lógicamente relacionadas que se encuentran distribuidas en diferentes espacios físicos o lógicos, interconectadas por una red de comunicaciones.

Sus principales características son:

1. Está formada por múltiples computadoras o nodos conectados en red.
2. Cada nodo tiene autonomía local y puede realizar operaciones de forma independiente en los datos que almacena.
3. Los datos están distribuidos entre los diferentes nodos, pero funcionan como una única base de datos lógica.
4. Permite el acceso a los datos desde cualquier nodo como si fueran locales, de forma transparente para el usuario.
5. Puede utilizar diferentes esquemas de distribución de datos, como replicación, particionamiento o híbrido.

Las BDD ofrecen ventajas como mayor disponibilidad, confiabilidad y eficiencia en el acceso a la información (rendimiento), así como la capacidad de expandirse fácilmente (escalabilidad). Sin embargo, también presentan desafíos en términos de consistencia de datos, complejidad de gestión (sobre todo sincronización), resolución de conflictos o seguridad en la comunicación.

Se utilizan pues en aplicaciones que requieren alto rendimiento, escalabilidad y confiabilidad. Por ejemplo, podríamos tener la gestión de un comercio electrónico global con nodos en América del Norte, Europa y Asia. Cada nodo permite la gestión de cada zona, pero los usuarios de una zona pueden interconectarse con la información de los nodos fuera de su zona.

Bases de datos relacionales

Las bases de datos relacionales(SGBD) son sistemas de almacenamiento y organización de datos que se caracterizan por:

1. **Estructura tabular:** Los datos se organizan en tablas compuestas por filas (registros) y columnas (atributos).
2. **Relaciones predefinidas:** Establecen conexiones lógicas entre diferentes tablas, permitiendo asociar datos relacionados. Estas relaciones se establecen empleando claves primarias (identificadores únicos para cada registro) y claves externas (foráneas) (referencias a claves primarias de otras tablas) para establecer y mantener relaciones.
3. **Lenguaje SQL:** Utilizan el ***Lenguaje de Consulta Estructurado (SQL - Structured Query Language)*** para manipular y consultar los datos.
4. **Integridad de datos:** Garantizan la consistencia y evitan la duplicidad de información.
5. **Modelo relacional:** Se basan en el modelo propuesto por Edgar Frank Codd en 1970, que representa los datos de forma intuitiva y directa.

6. **Flexibilidad:** Permiten acceder y relacionar datos de múltiples formas sin necesidad de reorganizar la estructura de la base de datos.
7. **Escalabilidad**: Pueden adaptarse desde sistemas pequeños de escritorio hasta grandes sistemas basados en la nube.

Las bases de datos relacionales son ampliamente utilizadas en diversos sectores empresariales debido a su eficiencia en el almacenamiento, recuperación y manipulación de datos estructurados. Proporcionan mecanismos para garantizar la coherencia y consistencia de las bases de datos, permiten las consultas complejas a través de operaciones del álgebra relacional y del lenguaje SQL, y poseen funcionalidades que garantizan la seguridad y la integridad de los datos como la definición de reglas y restricciones o el control de acceso a los datos a través de usuarios y roles.

Un ejemplo de base de datos relacional puede ser la gestión de los libros de una biblioteca. Podemos tener un servidor web donde alojamos una aplicación web de acceso a través de internet, y esta aplicación funciona usando una base de datos MySQL o mariaDB, con varias tablas relacionadas entre sí: libros, autores, socios de la biblioteca y préstamos. **La información básica de un ejemplar** (ID o identificación única, título, ISBN, sinopsis, género, año de publicación…) **se almacena en la tabla libros**, donde también reservamos un atributo para la identificación del autor. Esta identificación es la identificación única (o clave primaria) del autor en la tabla autores, donde se guarda el resto de la información del autor.

Comparativa entre tipos de bases de datos

	Bases de datos distribuidas (BDD)	Bases de datos relacionales (SGBD)
Rendimiento	**Ofrecen mejor rendimiento para consultas distribuidas y procesamiento paralelo**	**Pueden ser más eficientes para operaciones locales y consultas simples.**
Escalabilidad	**Altamente escalables, permiten añadir nodos fácilmente para aumentar la capacidad**	**Escalabilidad limitada, generalmente requieren actualización de hardware**
Confiabilidad	**Mayor confiabilidad debido a la replicación de datos y tolerancia a fallos**	**Pueden ser menos confiables al depender de un único punto de fallo**
Complejidad de gestión	**Mayor complejidad debido a la necesidad de gestionar múltiples nodos y mantener la consistencia**	**Generalmente más simples de administrar al estar centralizados.**

Aplicaciones adecuadas	**Ideales para empresas grandes, aplicaciones globales y sistemas que requieren alta disponibilidad**	**Adecuados para aplicaciones locales, pequeñas y medianas empresas, y sistemas con menor complejidad**

Las BDD son superiores en términos de escalabilidad, confiabilidad y rendimiento para grandes volúmenes de datos distribuidos, mientras que los SGBD tradicionales ofrecen una gestión más simple y son adecuados para aplicaciones locales menos complejas.

Ciberseguridad a nivel de usuario

La ciberseguridad es la práctica de proteger sistemas informáticos, redes, programas y datos contra amenazas, ataques digitales, accesos no autorizados y daños.

A nivel de usuario, implica salvaguardar la información personal, la privacidad, la identidad digital y proteger los dispositivos que conectamos a internet.

Amenazas comunes

- **Malware**: Software malicioso que daña o infecta sistemas, como virus, gusanos o troyanos.
- **Phishing**: Ataques que buscan obtener información confidencial haciéndose pasar por entidades confiables. Frecuentemente son mensajes SMS (smishing), correos electrónicos o sitios web falsos que solicitan al usuario datos sensibles como direcciones y cuentas bancarias.
    - El **pharming** (variación de phishing) es un tipo de ciberataque que redirige a los usuarios a sitios web fraudulentos sin su conocimiento o consentimiento, engañandolos y haciéndolos creer que están en el sitio web correcto (ejemplo, una copia fraudulenta de la página de tu banco).
- **Ransomware**: Secuestra datos o sistemas y exige un rescate para liberarlos.
- **Spyware:** software malicioso diseñado para infiltrarse en dispositivos informáticos sin el conocimiento ni consentimiento del usuario. Roba información comercial para enviarla a un tercero.
- **Ataques de denegación de servicio (DoS/DDoS):** Buscan colapsar servidores o sitios web mediante tráfico excesivo
- **Ingeniería social:** Manipulación psicológica para obtener información confidencial, bien haciéndose pasar por alguien confiable o bien usando otras tácticas psicológicas.
- **Inyección SQL:** Inserción de código malicioso en servidores SQL para acceder a información.
- **Man-in-the-middle:** Interceptación de comunicaciones entre dos partes. Pueden ser redes (por ejemplo, redes inalámbricas WiFi) imitando el nombre de redes conocidas con la esperanza de que el usuario se conecte por error a ellas, interceptando sus comunicaciones.
- **Spam**: Envío masivo de correos no deseados, a menudo con fines maliciosos.
- **Ataques de contraseña:** Intentos de adivinar o robar contraseñas de usuarios.

Riesgos personales usando redes

Los principales riesgos personales en el uso de internet y las redes sociales incluyen:

1. **Robo de identidad:** suplantación de identidad usando información personal compartida en línea para fines normalmente delictivos o ilícitos.

2. **Ciberacoso o ciberbullying:** Acoso a través de medios digitales, incluyendo mensajes ofensivos , chantajes y amenazas.
3. **Phishing y fraudes:** Intentos de obtener información confidencial o dinero mediante engaños.
4. **Exposición de información privada:** Compartir excesivamente datos personales que pueden ser mal utilizados.
5. **Riesgos de seguridad física:** Publicar ubicaciones en tiempo real puede exponer a robos o acoso físico.
6. **Daño a la reputación:** Publicaciones inapropiadas pueden afectar la imagen personal y profesional.
7. **Adicción a las redes sociales:** Uso compulsivo que afecta la vida cotidiana y las relaciones personales.
8. **Acceso a contenido inapropiado:** Especialmente peligroso para menores de edad.
9. **Pérdida de privacidad:** Empresas y terceros pueden acceder y utilizar datos personales sin consentimiento.
10. **Problemas de seguridad laboral:** Compartir información confidencial del trabajo puede tener consecuencias profesionales.
11. **Exposición a bulos y fake news:** influir en la opinión de las personas mediante engaños y mentiras, a veces muy elaboradas.
12. **Discursos de odio:** se entiende como una acción comunicativa que busca promover y alimentar prejuicios, estigmatización y discriminación hacia grupos históricamente marginados o personas individuales.

Medidas básicas de protección

Los usuarios individuales pueden tomar diversas medidas de protección contra amenazas y riesgos en internet. A continuación se presentan algunas recomendaciones clave:

1. Contraseñas Seguras: utiliza contraseñas largas y complejas, combinando letras mayúsculas, minúsculas, números y símbolos. No reutilices contraseñas en diferentes cuentas para evitar que un compromiso afecte a otras. Evita usar información personal predecible.

2. Autenticación de Dos Factores (2FA): configura la 2FA en tus cuentas para añadir una capa adicional de seguridad, utilizando algo que conoces (contraseña) y algo que tienes (teléfono móvil).

3. Actualizaciones de Software: mantén tu sistema operativo y aplicaciones actualizados para protegerte contra vulnerabilidades de seguridad.

4. Redes Wi-Fi Seguras: evita realizar actividades sensibles en redes Wi-Fi públicas. Si es necesario, utiliza una VPN para cifrar tu conexión.Asegura tu red doméstica con una contraseña fuerte y utiliza el cifrado WPA3 si es posible.

5. Navegación Segura: asegúrate de que los sitios web que visitas utilicen HTTPS para proteger tus datos. Instala extensiones de navegador que bloqueen rastreadores y publicidad maliciosa.

6. Gestión de la Privacidad en Redes Sociales: revisa y ajusta las configuraciones de privacidad en tus perfiles para controlar quién puede ver tu información. Sé cauteloso con la información personal que compartes en línea.

7. Educación sobre Phishing: Aprende a identificar correos electrónicos sospechosos y verifica siempre la autenticidad de las solicitudes antes de proporcionar información personal.

8. Uso de Antivirus, Antimalware y Cortafuegos: instala software antivirus y mantén un cortafuegos activo para proteger tu dispositivo contra malware y accesos no autorizados.

9. Copia de Seguridad Regular: realiza copias de seguridad periódicas de tus datos importantes para prevenir pérdidas en caso de ataques o fallos del sistema.

10. Control de Acceso a Dispositivos: utiliza contraseñas o métodos biométricos para bloquear el acceso a tus dispositivos móviles y computadoras.

11. Uso de certificados digitales o DNI electrónico, para autentificarse de forma segura y evitar suplantaciones.

Recuerda que todas estas medidas ayudan, pero es necesario mantenerse actualizado ya que la seguridad cibernética es un proceso en constante evolución. La actitud más segura es la de ser precavido y estar al tanto de las últimas amenazas y tendencias en ciberseguridad.

Para saber más: https://www.aepd.es/areas-de-actuacion/recomendaciones/medidas