

8

Sistemas informáticos emergentes

"A algunas personas les preocupa que la inteligencia artificial nos haga sentir inferiores, pero cualquier persona en su sano juicio debería tener un complejo de inferioridad cada vez que mira una flor."

Alan Kay (1940-), informático estadounidense y premio Turing en 2003



Conoce

1. Fundamentos de la inteligencia artificial
2. Tipos de inteligencia artificial
3. Impacto social de la inteligencia artificial. Los sesgos
4. Aplicaciones de la inteligencia artificial
5. Big data
6. Bases de datos distribuidas y bases de datos relacionales
7. La ciberseguridad a nivel de usuario

Resumen de la unidad

Actividades de refuerzo

1. Fundamentos de la inteligencia artificial

La **inteligencia artificial (IA)** es la capacidad que tiene una máquina de realizar funciones propias de los seres humanos.

Más allá de la capacidad de cálculo o la memoria, que los ordenadores pueden replicar fácilmente, la inteligencia artificial se refiere a otras capacidades, como la creatividad, el aprendizaje o la toma de decisiones de acuerdo con experiencias anteriores.

En la actualidad, la inteligencia artificial es una rama de la computación que desarrolla algoritmos muy eficientes que permiten a la máquina aprender y, así, dar respuesta a escenarios diferentes de aquellos para los que fueron creados.

Escanea este código para ver un vídeo en el que se muestra **cómo detecta y actúa un coche autónomo**.

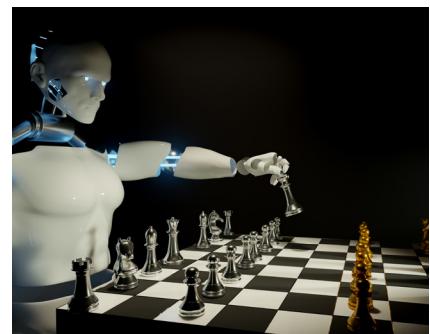


2. Tipos de inteligencia artificial

Podemos clasificar la inteligencia artificial de diferentes formas. Uno de los posibles enfoques es según su capacidad y su cognición. En este sentido debemos tener presentes algunos conceptos:

- **Máquinas reactivas.** Las máquinas reactivas son el tipo más básico de IA. Son sistemas de inteligencia artificial que se basan en respuestas reactivas directas a entradas específicas. No tienen memoria ni capacidad de aprendizaje, por lo que toman decisiones basadas únicamente en la entrada sin considerar el contexto o las experiencias pasadas.

Los sistemas basados en reglas y los sistemas expertos son ejemplos de máquinas reactivas. Por ejemplo, un robot esquiaobstáculos es una máquina reactiva.



- **Máquinas con memoria limitada.** Las máquinas con memoria limitada pueden almacenar información sobre su entorno y utilizarla para tomar decisiones. Tienen la capacidad de recordar información relevante durante un determinado período de tiempo. Estos sistemas pueden usar la información almacenada en su memoria para tomar decisiones más informadas y contextuales. Sin embargo, su capacidad de memoria es limitada y no poseen una comprensión profunda del pasado.

Los modelos de aprendizaje automático tradicionales, como los clasificadores bayesianos y las redes neuronales sin memoria a largo plazo, son ejemplos de sistemas con memoria limitada. Así, un sistema de reconocimiento facial puede almacenar información sobre las caras que ha visto anteriormente y utilizarla para identificar caras nuevas.





- **Teoría de la mente.** La teoría de la mente es la capacidad de comprender y atribuir estados mentales, como creencias, deseos e intenciones, a otros seres conscientes. En el contexto de la inteligencia artificial, la teoría de la mente implica que un sistema tenga la capacidad de comprender y modelar los estados mentales de los seres humanos para poder interactuar de manera más efectiva con ellos. Actualmente, la teoría de la mente es un área de investigación activa en la IA y se utiliza en aplicaciones como los asistentes virtuales y los chat-bots, así como en los llamados *agentes de negociación*, que pueden entender las intenciones de la otra parte y servirse de esta información para negociar un acuerdo favorable.

- **Autoconciencia.** La autoconciencia es la capacidad de un sistema para tener conocimiento y comprensión de sí mismo. En el contexto de la inteligencia artificial, la autoconciencia implica que un sistema sea consciente de su propia existencia, sus capacidades y sus limitaciones. Las máquinas autoconscientes pueden pensar por sí mismas y tomar decisiones sin la ayuda de un humano. Aún no existen, pero son un objetivo de investigación. La autoconciencia en las máquinas es un tema complejo y controvertido, y actualmente no se ha logrado desarrollar sistemas de IA plenamente autoconscientes en el sentido humano.

Es importante tener en cuenta que estos fundamentos representan diferentes niveles de inteligencia y conciencia, y que la mayoría de los sistemas de inteligencia artificial actuales se encuentran en los niveles más bajos de la escala.

La IA es un campo complejo y en rápida evolución. A medida que esta tecnología continúa desarrollándose, iremos viendo cada vez más aplicaciones más sofisticadas en nuestras vidas cotidianas.

3. Impacto social de la inteligencia artificial. Los sesgos

Escanea este código para ver el vídeo “Machine learning para intentar traducir el lenguaje de signos en tiempo real”, del canal BlogThinkBig.



La inteligencia artificial está teniendo un impacto muy importante en nuestra sociedad. Vamos a ver algunos de sus aspectos positivos, pero también los peligros y los sesgos a los que nos enfrentamos:

■ Impacto positivo

- **Integración** de personas con alguna **minusvalía**. Por ejemplo, para los sordomudos, hay inteligencias artificiales capaces de “leer” los movimientos de las manos y poner voz a quienes utilizan un lenguaje de signos. Para las personas ciegas o con visión reducida, la aplicación Seeing AI, de Microsoft, puede ver lo que hay a su alrededor por medio de una cámara y proporcionarles una descripción, o leerles textos.
- Aumento de la **productividad** y de la **calidad** de producción. Hay robots que son capaces de trabajar 24 horas al día de forma precisa en tareas industriales.
- Desarrollo de las **creaciones artísticas**. Están apareciendo todo tipo de aplicaciones inteligentes capaces de escribir textos, dibujar imágenes, componer música, etc.
- **Búsquedas** inteligentes, predictivas y más precisas. Algunas inteligencias permiten mantener conversaciones casi reales (como ChatGPT).

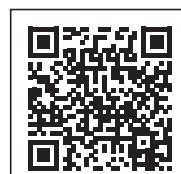
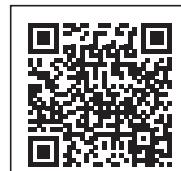
Impacto negativo

- Uso fraudulento de los **datos personales**, ya sea por filtraciones o por fugas de seguridad.
- Falsificaciones** de fotos y vídeos con malas finalidades, como por ejemplo suplantar la personalidad de alguien. La aplicación de vídeo FakeApp, usando el aprendizaje automático, permite a sus usuarios cambiar las caras de las personas en sus vídeos.
- Riesgo de desaparición de **empleos**. Algunos expertos opinan que podrían perderse muchos puestos de trabajo. Por ejemplo, Juan Ignacio Rouyet cifró el impacto en un 14% a escala mundial y opina que la IA no siempre es posible ni deseable, ya sea por cuestiones de eficiencia, ética o legalidad.
- Modificaciones en el **comportamiento** de las personas. Por ejemplo, puede darse el caso de niños que trasladan al trato con seres humanos el comportamiento que tienen con las máquinas y los robots.
- Errores** de funcionamiento. Las inteligencias artificiales no son perfectas y pueden acarrear problemas. Por ejemplo, en el reconocimiento facial, un error puede llevar a castigar o multar a la persona equivocada. Entre los errores de funcionamiento de la IA son especialmente importantes los **sesgos**.

Suplantación de identidades

Con la IA es posible crear **deepfakes** (vídeos falsos de personas que aparentemente son reales) y utilizarlos con malas finalidades.

Escanea estos códigos para ver dos ejemplos de deepfakes.



Sesgos de la inteligencia artificial

Los **sesgos** son aquellos errores sistemáticos en que se incurre cuando, al hacer muestreos o ensayos, se seleccionan o favorecen unas respuestas frente a otras.

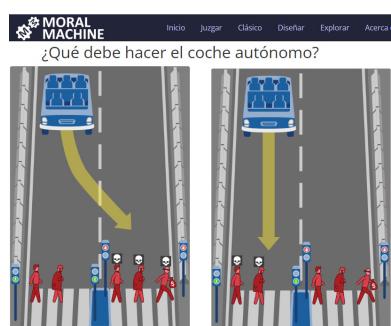
Como acabas de ver, los sistemas de inteligencia artificial son capaces de aprender, pero su aprendizaje está basado en una serie de modelos sobre los que son entrenados. Si, por alguna razón, estos modelos se limitan a una característica determinada, los resultados no serán los deseables. Por ejemplo, en los sistemas de reconocimiento facial, si entrenamos al sistema únicamente con personas de piel blanca, la inteligencia artificial así creada no será capaz de reconocer caras de personas con otros tonos de piel.

Esto fue lo que le sucedió a Joy Buolamwini, una científica de origen ghanés, que se dio cuenta de que el sistema de reconocimiento facial fallaba en un alto porcentaje cuando se trataba de identificar a mujeres de piel oscura. ¿Te imaginas que tu móvil no reconociese tu cara por ser muy moreno? ¿Te imaginas que una inteligencia artificial te rechazara para un puesto de trabajo por haber sido entrenada con imágenes de un único sexo?

Los sistemas de IA sesgados están condicionados por variables sensibles como el grupo étnico, la identidad sexual, el género, la religión, el pensamiento político, etc. Todos ellos provocan que se produzcan resultados erróneos y/o injustos.

Los sesgos pueden ser introducidos en los datos que se utilizan al entrenar a la IA (por ejemplo, si están mal etiquetados o si no se tienen en cuenta todas las posibilidades), en las variables (al tomar unas variables equivocadas o al usar menos variables de las necesarias), en el diseño de la IA o en la configuración del sistema.

Tenemos que ser capaces de detectar esos sesgos, que pueden haberse producido con una cierta intencionalidad o surgir sin intención.



Moral Machine es una plataforma en línea que recopila distintas perspectivas sobre las decisiones que toma una máquina inteligente.

4. Aplicaciones de la inteligencia artificial

La inteligencia artificial tiene **aplicaciones** en múltiples campos, entre ellos los siguientes:



- **Asistentes personales virtuales.** Son sistemas que nos permiten, mediante el reconocimiento de voz, dar órdenes o iniciar la ejecución de determinadas acciones de forma automática en nuestras casas, teléfonos móviles, etc. Por ejemplo: Alexa, Siri o Cortana.



- **Asistentes de voz para empresas.** Por ejemplo, los chatbots (o bots conversacionales), que interactúan con los usuarios por medio de respuestas automáticas y permiten, mediante el reconocimiento de voz, llevar a cabo operaciones de consulta o comerciales sin necesidad de una persona física.



- **Transporte.** Mediante la inteligencia artificial podemos saber al momento dónde se encuentra un autobús y el tiempo que tardará en llegar; las aplicaciones como Google Maps o Waze analizan el tráfico y nos indican la mejor ruta para llegar a nuestro destino; los coches autónomos son capaces de aprender sobre la marcha por dónde circular, reconociendo los objetos y señales; etc.



- **Reconocimiento facial.** No sólo los móviles se desbloquean o sacan fotos utilizando el reconocimiento facial. También la policía de muchos países emplea cámaras especiales para reconocer a las personas y encontrar así delincuentes.



- **Medicina.** La inteligencia artificial permite obtener diagnósticos certeros y precoces que mejoran las posibilidades de supervivencia de los pacientes.



- **Selección de contenidos** en redes sociales, aplicaciones de música, televisión a la carta, etc., para mostrar al usuario contenidos de su gusto y preferencia.



- **Comercio.** Con la inteligencia artificial se pueden hacer pronósticos de ventas para conocer la acogida que tendrá un determinado producto.

5. Big data

El **big data** es el conjunto de datos extremadamente grandes y complejos que no pueden ser fácilmente gestionados, procesados o analizados mediante herramientas tradicionales de procesamiento de datos.

El big data se utiliza en una amplia gama de industrias y campos, como el marketing, la salud, las finanzas, la investigación científica, la logística o la seguridad. Para manejar los datos se utilizan técnicas y tecnologías como el almacenamiento distribuido, el procesamiento paralelo, el análisis de datos en tiempo real, el aprendizaje automático o la inteligencia artificial.

Estos conjuntos de datos se caracterizan por unos atributos conocidos como las **siete V**: volumen, variedad, velocidad, veracidad de los datos, viabilidad, visualización de los datos y valor.

- **Volumen.** El big data se caracteriza por tener un volumen masivo de datos. Esto implica que la cantidad de datos generados y almacenados es tan grande que los enfoques tradicionales no son suficientes para manejarlos. Los datos pueden provenir de diversas fuentes, como redes sociales, sensores, transacciones comerciales, registros de actividad, etc.
- **Variedad.** El big data puede estar compuesto por diferentes tipos y formatos de datos (como texto, imágenes, videos, audios...) y datos estructurados o no estructurados. Los datos pueden provenir de diversas fuentes y estar en diferentes formatos, lo que plantea desafíos para su procesamiento y análisis.
- **Velocidad.** En el entorno del big data, los datos se generan a una velocidad alta y constante. Esto significa que deben ser procesados y analizados en tiempo real o con una mínima latencia para obtener información valiosa y relevante de ellos.
- **Veracidad.** La veracidad está asociada a la calidad y confiabilidad de los datos. Los datos a menudo pueden contener información incompleta, inexacta o no confiable debido a su gran volumen y a la diversidad de fuentes. Por lo tanto, es importante disponer de mecanismos y procesos que permitan evaluar y garantizar la veracidad de los datos utilizados en el análisis.
- **Viabilidad.** Es la capacidad de procesar y analizar los conjuntos de big data utilizando las herramientas y tecnologías disponibles. Esto incluye la infraestructura de almacenamiento, las técnicas de procesamiento, los algoritmos de análisis y la capacidad de cómputo necesaria para manejar con eficiencia el volumen y la variedad de datos.
- **Visualización.** La visualización de los datos implica la representación gráfica y visual de los patrones, las relaciones y las tendencias dentro del conjunto de big data. La visualización efectiva permite comprender mejor los datos, identificar patrones ocultos y comunicar información de manera clara y accesible.
- **Valor.** Se refiere a la capacidad de extraer información útil y relevante de los conjuntos de datos. El objetivo final del análisis del big data es generar conocimientos que puedan conducir a decisiones informadas, mejoras operativas, descubrimiento de oportunidades y valor añadido para las organizaciones.



Estas características fundamentales del big data (volumen, velocidad, variedad, veracidad, viabilidad, visualización y valor) proporcionan un marco para comprender los desafíos y oportunidades asociados con el análisis de grandes conjuntos de datos. Al considerar estas características, las organizaciones pueden implementar estrategias y tecnologías adecuadas para aprovechar al máximo el potencial del big data.



6. Bases de datos distribuidas y bases de datos relacionales

Los conceptos de base de datos distribuida y base de datos relacional están relacionados en el ámbito de la gestión de datos pero son distintos. A continuación, veremos brevemente en qué consiste cada uno de ellos.



Bases de datos distribuidas

Una **base de datos distribuida** es un sistema en el que los datos se almacenan en múltiples ubicaciones físicas y están interconectados mediante una red de comunicación. En una base de datos de este tipo, los datos se dividen y se almacenan en diferentes servidores o nodos, y cada nodo puede ejecutar operaciones locales en los datos que almacena. Además, los nodos pueden comunicarse y coordinarse para llevar a cabo operaciones conjuntas, como consultas distribuidas o transacciones en varios nodos.



Las bases de datos distribuidas ofrecen ventajas como la escalabilidad, el rendimiento y la disponibilidad. Al distribuir los datos, es posible manejar grandes volúmenes de información y distribuir la carga de trabajo entre los nodos, lo que puede mejorar el rendimiento y evitar puntos únicos de fallo. Sin embargo, también presentan ciertos desafíos, como la gestión de la sincronización y la consistencia de los datos entre los nodos, la resolución de conflictos o la seguridad de la comunicación.

Las bases de datos distribuidas se utilizan para aplicaciones que requieren un alto rendimiento, escalabilidad y confiabilidad.

Bases de datos relacionales

Las **bases de datos relacionales** son un tipo de sistema de gestión de bases de datos (SGBD) que se basa en el modelo relacional de tablas. En este modelo, los datos se organizan en tablas (compuestas por filas y columnas) y se establecen relaciones entre ellas utilizando claves primarias y claves foráneas. Las bases de datos relacionales usan el lenguaje SQL (*structured query language*) para realizar consultas y manipulaciones de datos.

Las bases de datos relacionales son ampliamente utilizadas debido a su estructura flexible y su capacidad para mantener la integridad de los datos. Proporcionan mecanismos para garantizar la coherencia y consistencia de los datos y admiten consultas complejas por medio de operaciones de álgebra relacional y SQL. Además, los SGBD relacionales ofrecen funciones para garantizar la seguridad y la integridad de los datos, como la gestión de usuarios y roles o la definición de restricciones y reglas.



En resumen, las bases de datos distribuidas se refieren a la distribución física de los datos en varios nodos interconectados, mientras que las bases de datos relacionales se basan en el modelo relacional y organizan los datos en tablas con relaciones definidas.

Ambos conceptos son relevantes en el campo de la gestión de datos y se utilizan en diferentes contextos y escenarios según las necesidades y requisitos específicos de cada aplicación.

	Base de datos distribuida	Base de datos relacional
Rendimiento	Alto	Puede no ser tan alto
Escalabilidad	Muy escalable	Puede no ser tan escalable
Confiabilidad	Altamente confiable	Puede no ser tan confiable
Complejidad de administración	Alta	Más fácil de administrar
Aplicaciones adecuadas	Aplicaciones que requieren un alto rendimiento, escalabilidad y confiabilidad	Aplicaciones que son más sencillas y no requieren un alto rendimiento

7. La ciberseguridad a nivel de usuario

La **ciberseguridad** es el conjunto de prácticas, herramientas y medidas que se implementan para proteger los sistemas informáticos y los datos contra amenazas, ataques y accesos no autorizados.

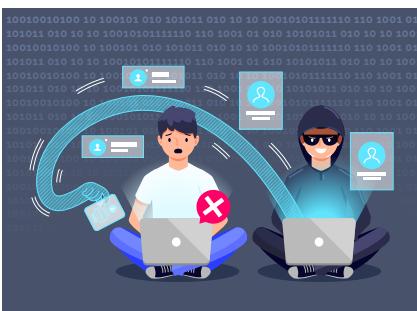
A nivel de usuario, implica salvaguardar la información personal, la privacidad, la identidad digital y los dispositivos conectados a Internet.

Vamos a ver las amenazas más comunes y algunas medidas básicas de protección en ciberseguridad a nivel de usuario:

■ Amenazas comunes

Existen diversas amenazas a las que los usuarios pueden estar expuestos en el ámbito cibernético. Algunas de las más comunes incluyen:

- **Malware.** Es un software malicioso diseñado para dañar, manejar o robar información de los sistemas, como por ejemplo virus, troyanos, ransomware o spyware.
- **Phishing.** Mediante esta técnica, los atacantes intentan engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos, mensajes o sitios web falsos. Si lo hacen por SMS se llama *smishing*.
- **Pharming.** Esta práctica consiste en redirigir un nombre de dominio a otra máquina distinta, de forma que un usuario que introduzca una URL acceda a la página web del atacante. De este modo, por ejemplo, éste puede suplantar una página web de un banco para obtener claves de la víctima.
- **Ataques de fuerza bruta.** Consisten en intentos repetitivos y automatizados para adivinar contraseñas o claves de acceso mediante la prueba de múltiples combinaciones.
- **Ataques de ingeniería social.** Implican manipular a los usuarios para obtener información confidencial, generalmente haciéndose pasar por una entidad confiable o utilizando tácticas psicológicas.
- **Ataque man in the middle.** Existen atacantes que imitan el nombre de una red cercana o de nombre conocido, con el objetivo de que alguien se conecte por error a ella, y, una vez que un usuario está conectado, pueden interceptar sus comunicaciones y robarle información pasando desapercibidos. También se llama *ataque de intermediario*.



Ataques a la persona

Los daños a la máquina no dejan de ser daños materiales, pero los daños causados a las personas permanecen en el tiempo y trascienden a otros aspectos de la vida.

Algunas de las principales amenazas a las personas son:

- El **ciberbullying** o **ciberacoso**, que es un tipo de acoso que consiste en amenazas, chantajes, etc., entre iguales a través de Internet, el teléfono móvil o los videojuegos
- Las **fake news** y los **bulos**
- Los **discursos de odio**
- El **acceso a comunidades peligrosas** que publican contenidos de riesgo
- La **suplantación de identidad**

Escanea este código para ver el “**Catálogo de medidas preventivas y herramientas para proteger la privacidad**” de la web de la Agencia Española de Protección de Datos.



■ Medidas básicas de protección

Algunas medidas básicas de protección que los usuarios pueden adoptar para fortalecer su seguridad cibernética son:

1. **Mantener actualizado el software.** Asegúrate de tener instaladas las últimas actualizaciones de tu sistema operativo y de tus aplicaciones y programas, ya que suelen incluir correcciones de seguridad importantes.
2. **Utilizar contraseñas fuertes.** Crea contraseñas únicas y robustas para cada cuenta, que combinen letras mayúsculas y minúsculas, números y símbolos. Evita utilizar información personal predecible y considera el uso de administradores de contraseñas.
3. **Ser cauteloso con los correos electrónicos y los enlaces sospechosos.** No abras ni descargas archivos adjuntos de fuentes no confiables. Ten cuidado con los enlaces cuando te soliciten información personal en un correo electrónico, un mensaje o una red social.
4. **Utilizar software de seguridad.** Instala y mantén actualizado un software antivirus y antimalware confiable en tus dispositivos.
5. **Hacer copias de seguridad.** Haz copias de seguridad periódicas de tus archivos importantes en un dispositivo de almacenamiento externo o en la nube. Esto te ayudará a recuperar los datos en caso de pérdida o daño.
6. **Configurar la privacidad en redes sociales.** Ajusta las configuraciones de privacidad en tus cuentas de redes sociales para limitar la información compartida y controlar quién puede acceder a tu perfil.
7. **Usar certificados digitales o el DNI electrónico** para autenticarte de manera segura y evitar suplantaciones.
8. **Mantener cifrados los contenidos de tus dispositivos móviles**, de forma que sólo pueda acceder a ellos quien conozca la clave de descifrado.
9. **Mantenerse informado.** Estate al tanto de las últimas tendencias y amenazas en ciberseguridad. Adopta una actitud vigilante y adquiere conocimientos sobre prácticas seguras en línea.

Recuerda que la seguridad cibernética es un proceso en constante evolución. Además de estas medidas básicas, existen muchas otras prácticas y herramientas que pueden ayudarte a proteger tu seguridad y privacidad.

1. Fundamentos de la inteligencia artificial

- La **inteligencia artificial (IA)** es la capacidad que tiene una máquina de realizar funciones propias de los seres humanos.

2. Tipos de inteligencia artificial

- Debemos tener presentes los conceptos de **máquinas reactivas, máquinas con memoria limitada, teoría de la mente y autoconciencia**.

3. Impacto social de la inteligencia artificial. Los sesgos

- **Impactos positivos:** integración de personas con alguna minusvalía; aumento de la productividad y de la calidad de producción; desarrollo de las creaciones artísticas; búsquedas inteligentes, predictivas y más precisas.
- **Impactos negativos:** uso fraudulento de los datos personales; falsificaciones de fotos y vídeos con malas finalidades; riesgo de desaparición de empleos; modificaciones en el comportamiento de las personas; errores de funcionamiento.
- Los **sesgos** son aquellos errores sistemáticos en que se incurre cuando, al hacer muestrazos o ensayos, se seleccionan o favorecen unas respuestas frente a otras.

4. Aplicaciones de la inteligencia artificial

- La inteligencia artificial tiene **aplicaciones** en múltiples campos: asistentes personales virtuales, asistentes de voz para empresas, transporte, reconocimiento facial, medicina, selección de contenidos, comercio, etc.

5. Big data

- El **big data** es el conjunto de datos extremadamente grandes y complejos que no pueden ser fácilmente gestionados, procesados o analizados mediante herramientas tradicionales de procesamiento de datos.
- Estos conjuntos de datos se caracterizan por unos atributos conocidos como las **siete V**: volumen, variedad, velocidad, veracidad de los datos, viabilidad, visualización de los datos y valor.

6. Bases de datos distribuidas y bases de datos relacionales

- Una **base de datos distribuida** es un sistema en el que los datos se almacenan en múltiples ubicaciones físicas y están interconectados mediante una red de comunicación.
- Las **bases de datos relacionales** son un tipo de sistema de gestión de bases de datos que se basa en el modelo relacional de tablas.

7. La ciberseguridad a nivel de usuario

- La **ciberseguridad** es el conjunto de prácticas, herramientas y medidas que se implementan para proteger los sistemas informáticos y los datos contra amenazas, ataques y accesos no autorizados.
- Las **amenazas más comunes** son: malware, phishing, pharming, ataques de fuerza bruta, ataques de ingeniería social y ataque man in the middle.

ACTIVIDADES DE REFUERZO

Inteligencia artificial

1. ♦ Explica en qué consisten las máquinas reactivas y pon un ejemplo.
2. ♦ Explica en qué consisten las máquinas con memoria limitada y pon un ejemplo.
3. ♦ ¿Qué son la teoría de la mente y la autoconciencia en el ámbito de la IA? Pon un ejemplo de cada una.
4. ♦♦ Señala cinco impactos positivos de la IA en la sociedad. Pon un ejemplo concreto para cada caso e indica cómo te podría afectar a ti en la vida diaria.
5. ♦♦ Señala cinco impactos negativos de la IA en la sociedad. Pon un ejemplo concreto para cada caso e indica cómo te podría afectar a ti en la vida diaria.
6. ♦ ¿Qué son los sesgos?
7. ♦♦♦ Describe ocho tipos de sesgos que existan en la sociedad en la que vivimos, cuatro de ellos que no tengan relación con el mundo cibernético o la IA y otros cuatro que sí la tengan.
8. ♦ Indica diez aplicaciones de la IA.
9. ♦♦ Describe tres aplicaciones que puede tener la IA en tu entorno más cercano (haciendo un buen uso de ella).

Big data

10. ♦ ¿Qué es el big data?
11. ♦ Describe brevemente los siete atributos principales del big data (las siete V).
12. ♦♦ Reflexiona sobre los atributos del big data. ¿Cuáles son los tres que te parecen más importantes? ¿Por qué?
13. ♦ ¿Qué es una base de datos distribuida? ¿Y una base de datos relacional?

Ciberseguridad

14. ♦ Explica en qué consisten el malware y el phishing.
15. ♦ Explica en qué consisten el pharming y los ataques de fuerza bruta.
16. ♦ Explica en qué consisten los ataques de ingeniería social y el ataque man in the middle.
17. ♦ Haz un resumen de las principales medidas de protección que debes adoptar para mantener tu seguridad cibernética.

Investigación

18. ♦♦ Consulta la guía *Privacidad y seguridad en Internet* del Instituto Nacional de Ciberseguridad (INCIBE) y elabora en Canva una infografía con los 15 consejos y recomendaciones que consideres más importantes.



Escanea este código para ver la guía **Privacidad y seguridad en Internet**, del Instituto Nacional de Ciberseguridad (INCIBE).



19. ♦♦ Lee el artículo "Sin privacidad no hay ciberseguridad", de la web de la AEPD, y selecciona al menos doce tipos de ataques o riesgos. Después de entender bien en qué consiste cada uno de ellos, elabora en Canva una infografía con dos columnas: en la primera, describe la técnica de ataque o el tipo de riesgo, y, en la otra, una medida de protección que podrías utilizar.

Escanea este código para acceder al artículo **"Sin privacidad no hay ciberseguridad"**, de la web de la Agencia Española de Protección de Datos (AEPD).

