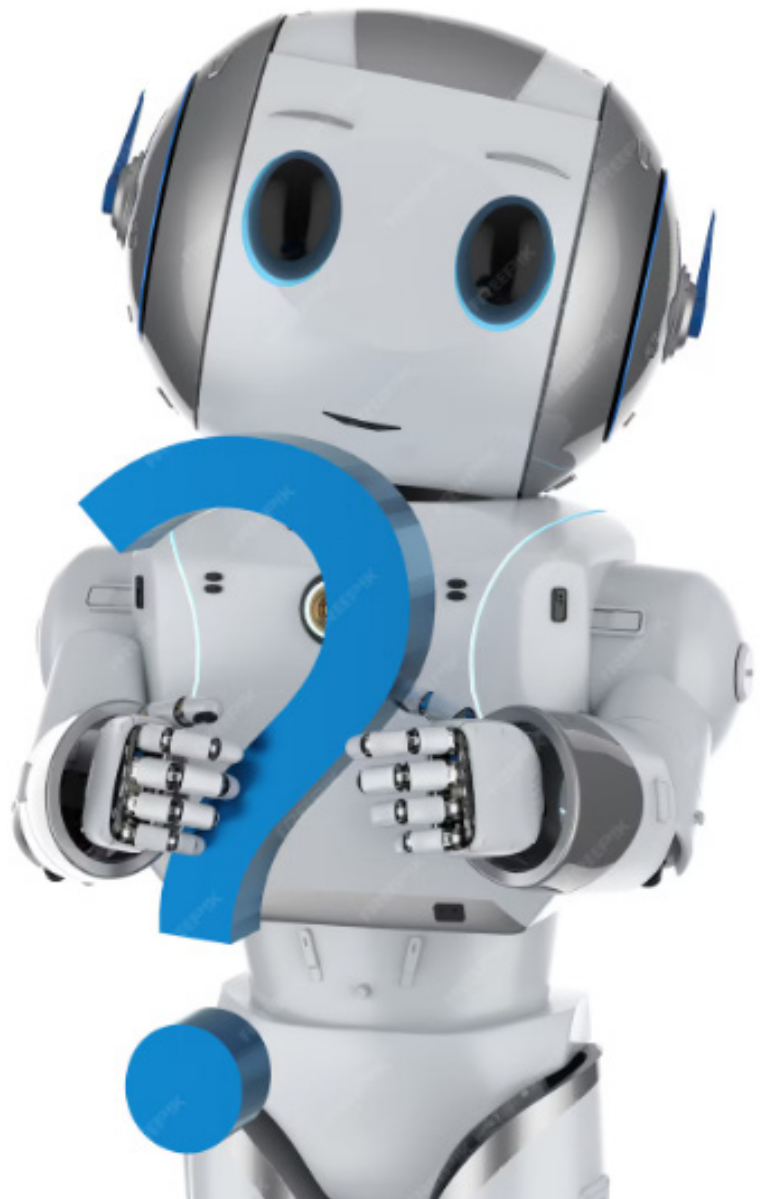


¿QUIERES ENTENDER MEJOR LA **INTELIGENCIA ARTIFICIAL?**

Aquí encontrarás los términos básicos que necesitas para moverte con seguridad en este nuevo mundo digital. Preparamos un glosario claro, completo y pensado para que cualquier persona —sin importar su nivel técnico— pueda comprender cómo funciona la IA, sus conceptos esenciales y sus aplicaciones prácticas.



**Descarga el glosario en PDF y
consérvalo como guía de
consulta permanente.**

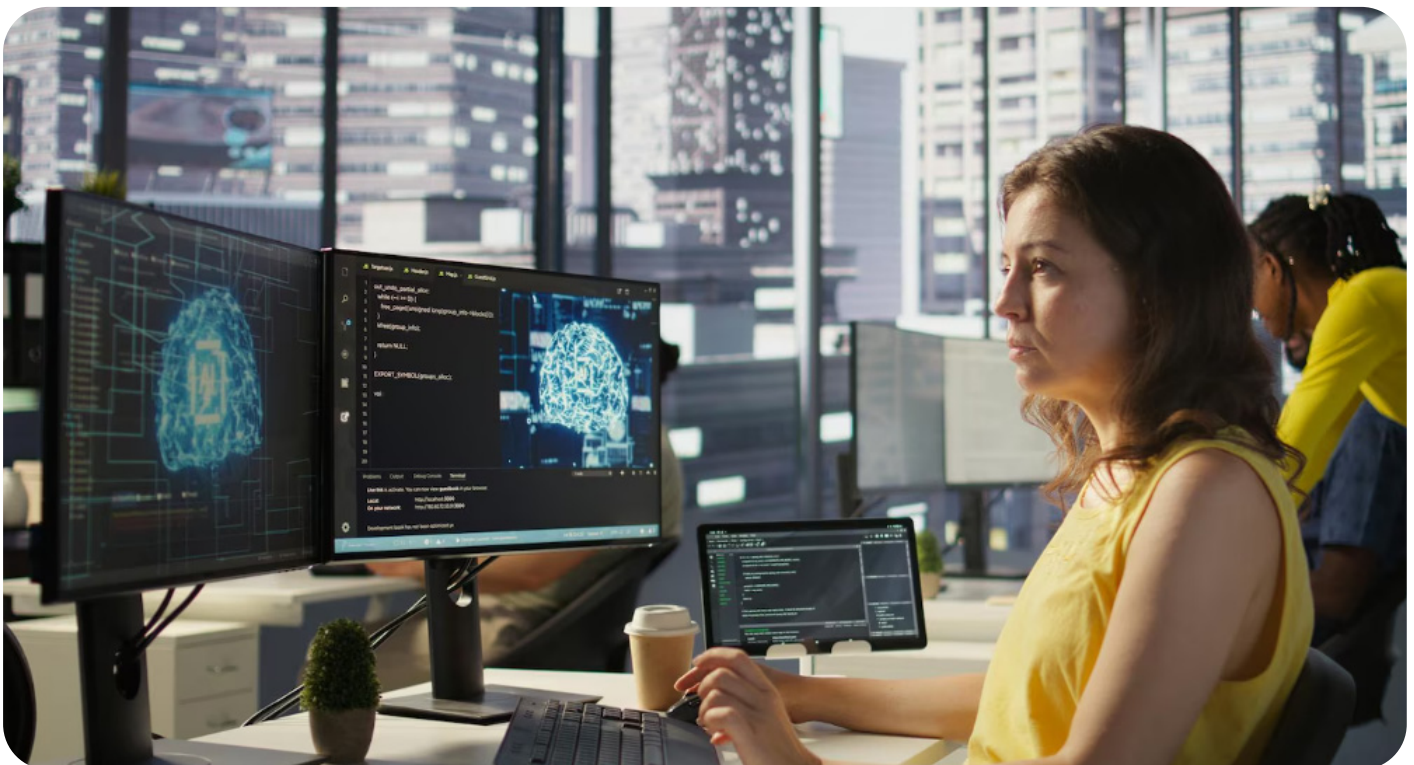
CONCEPTOS FUNDAMENTALES

IA (Inteligencia Artificial)

Campo de la informática que busca desarrollar sistemas capaces de aprender, razonar y tomar decisiones, imitando o ampliando la inteligencia humana.

IA generativa

Subcampo de la IA que crea contenido nuevo —texto, imágenes, audio, video o código— a partir de patrones aprendidos de datos existentes.



Modelo

Estructura matemática que aprende de los datos. Su función es reconocer patrones, generar predicciones o producir contenido.

LLM (Large Language Model)

Modelo de lenguaje de gran escala entrenado con enormes cantidades de texto. Comprende, predice y genera lenguaje humano. Ejemplo: GPT-5.

PROCESOS Y MECANISMOS

Entrenamiento

Etapa en la que el modelo aprende de millones de ejemplos. Ajusta sus parámetros internos para minimizar errores y mejorar la precisión.

Inferencia

Uso del modelo ya entrenado para generar respuestas o resultados en tiempo real.

Modelo de inferencia

Versión del modelo utilizada para ejecutar tareas y responder consultas, sin seguir aprendiendo.



Modelo de razonamiento

Modelo avanzado que no solo predice respuestas, sino que puede analizar causas, relaciones y consecuencias antes de responder.

Tokens

Unidades mínimas en que el modelo divide el texto (pueden ser palabras, sílabas o signos). Los modelos calculan capacidad y costo por número de tokens.

Ventana de conversación (o ventana de contexto)

Cantidad máxima de tokens que un modelo puede “recordar” dentro de una conversación o texto.

Por ejemplo, si un modelo tiene una ventana de 128.000 tokens, puede considerar esa cantidad de palabras antes de “olvidar” el inicio.



ELEMENTOS DE FUNCIONAMIENTO

Prompt

Instrucción o texto que el usuario envía a la IA. La calidad del resultado depende de su claridad y contexto.

Rol

Papel o función que asume la IA en una interacción: profesor, periodista, analista, etc. Define el tono y la profundidad de las respuestas.

Enfoque

Perspectiva o modo con el que el modelo interpreta una tarea. Puede ser técnico, analítico, narrativo o creativo.



Límites

Restricciones éticas, técnicas o de diseño del modelo. Marcan lo que no puede hacer, como acceder a datos privados, ejecutar acciones reales o emitir juicios humanos.

Memoria

Capacidad del modelo para recordar información previa. Puede ser temporal (solo durante la conversación) o persistente (entre sesiones).



One-shot prompting

Consiste en **dar un solo ejemplo** dentro del prompt para guiar al modelo.

Sirve cuando quieres mostrarle el **formato o estilo exacto** que esperas en la respuesta.

Ejemplo: “Traduce el siguiente texto al inglés: ‘La IA está transformando el periodismo’. Ejemplo: ‘La educación impulsa el progreso’ → ‘Education drives progress’.”

Few-shot prompting

Técnica que incluye **varios ejemplos (dos o más)** antes de la instrucción principal.

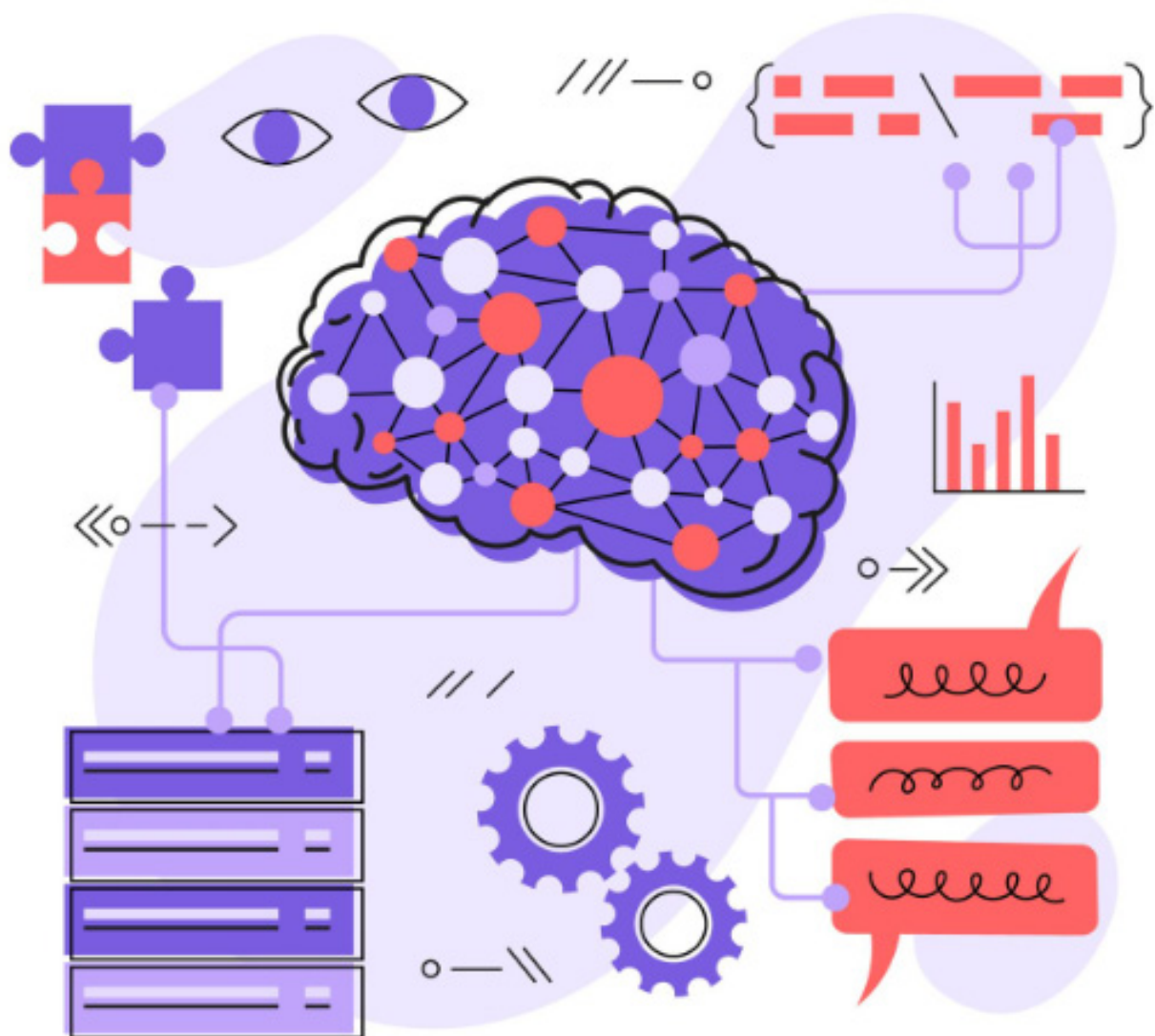
Le ayuda al modelo a **aprender el patrón o estilo** que debe seguir sin necesidad de entrenamiento adicional.

Ejemplo: mostrar tres titulares bien escritos antes de pedirle que redacte uno nuevo en el mismo tono.

Cadena de pensamiento (Chain of Thought)

Consiste en pedirle al modelo que **muestre su razonamiento paso a paso** antes de dar la respuesta final. Aumenta la precisión en tareas que requieren lógica o análisis.

Ejemplo: “Explica paso a paso cómo llegas a la conclusión antes de responder.”



ESTRUCTURA DE DATOS

Key (clave)

Etiqueta o identificador que permite acceder a un dato.
Ejemplo: en {"nombre": "Rosa"}, “nombre” es la key.

Value (valor)

Dato asociado a una clave. En el ejemplo anterior, “Rosa” es el value.

Query

Consulta o solicitud de información al modelo o a una base de datos.



TÉRMINOS COMPLEMENTARIOS

Embedding

Representación numérica de una palabra o idea en un espacio de muchas dimensiones. Permite medir similitudes semánticas entre textos.

Fine-tuning (ajuste fino)

Reentrenamiento de un modelo con datos específicos para adaptarlo a un contexto determinado (por ejemplo, salud, educación o periodismo).

Agente

Sistema autónomo basado en IA que puede percibir, razonar y actuar para cumplir objetivos. Combina modelos, herramientas y memoria.

Pipeline

Secuencia de pasos que conectan procesos de IA

(por ejemplo:
limpiar datos →
entrenar modelo → inferir
→ evaluar resultados).

Parámetro

Valor interno del modelo ajustado durante el entrenamiento. Cuantos más parámetros, mayor capacidad de aprendizaje.



CIBERSEGURIDAD

Ciberseguridad

Conjunto de prácticas, herramientas y políticas destinadas a **proteger sistemas, redes, datos y usuarios** frente a ataques, accesos no autorizados o daños digitales. Su objetivo es garantizar la **confidencialidad, integridad y disponibilidad** de la información.



Ciberdelito (o cibercrimen)

Actividad ilícita realizada mediante medios digitales, como robo de información, suplantación de identidad, fraudes, o ataques a infraestructuras tecnológicas.

Amenaza digital

Riesgo o evento con potencial de causar daño a un sistema informático. Puede ser intencional (hackeo) o accidental (error humano).

Vulnerabilidad

Debilidad o falla de seguridad en un sistema, red o usuario que puede ser aprovechada por atacantes.

Ataque informático (Cyber Attack)

Acción deliberada para interrumpir, dañar o tomar control de sistemas digitales. Ejemplos: phishing, ransomware o ataques DDoS.

Phishing

Estrategia de engaño en la que se envían mensajes falsos que simulan ser legítimos para robar datos personales o contraseñas.

Malware

Software malicioso diseñado para infiltrarse en un sistema y causar daño, robar información o tomar el control.

Incluye virus, troyanos y ransomware.



Ransomware

Tipo de malware que bloquea el acceso a los datos y exige un pago (rescate) para liberarlos.

Ingeniería social

Técnica de manipulación psicológica que busca que una persona revele información confidencial o realice acciones inseguras.

Autenticación

Proceso que **verifica la identidad** de un usuario o sistema antes de permitir el acceso. Puede basarse en algo que el usuario sabe (contraseña), tiene (token) o es (huella digital).



Autorización

Etapa que **determina los permisos** o acciones que puede realizar un usuario autenticado. Controla qué recursos puede ver o modificar.

Principio de mínimo privilegio

Norma que establece que cada usuario o proceso debe tener **solo los permisos necesarios** para realizar sus funciones, reduciendo riesgos de abuso o error.



Confidencialidad

Garantiza que la información solo sea accesible para usuarios autorizados, protegiendo la privacidad y evitando divulgaciones indebidas.

Integridad

Asegura que los datos **no sean alterados** o manipulados sin autorización, preservando su exactitud y confiabilidad.

Disponibilidad

Principio que garantiza que los sistemas y datos estén **accesibles cuando se necesiten**, mediante planes de contingencia y redundancia.

Cifrado

Proceso que transforma los datos en un formato ilegible, accesible solo con una clave o código autorizado.



Zero Trust (Confianza Cero)

Modelo de seguridad que asume que **ningún usuario o dispositivo es confiable por defecto**, incluso dentro de la red. Requiere autenticación y autorización continua.

Ciberhigiene

Conjunto de hábitos y buenas prácticas personales para mantener la seguridad digital, como actualizar contraseñas y evitar redes públicas inseguras.

Auditabilidad

Capacidad de un sistema para **registrar y verificar** todas las acciones realizadas sobre los datos o recursos.

Permite rastrear quién hizo qué, cuándo y cómo, garantizando **transparencia, trazabilidad y control**.

Es fundamental para detectar incidentes, corregir errores y cumplir con normas de seguridad y protección de datos.



No repudio

Principio de la seguridad de la información que asegura que una persona **no pueda negar la autoría** de una acción o comunicación digital.

Se apoya en **firmas digitales, certificados y sellos de tiempo**, que garantizan la autenticidad y responsabilidad de las operaciones realizadas.

Su objetivo es evitar disputas y proteger la integridad de las transacciones electrónicas.