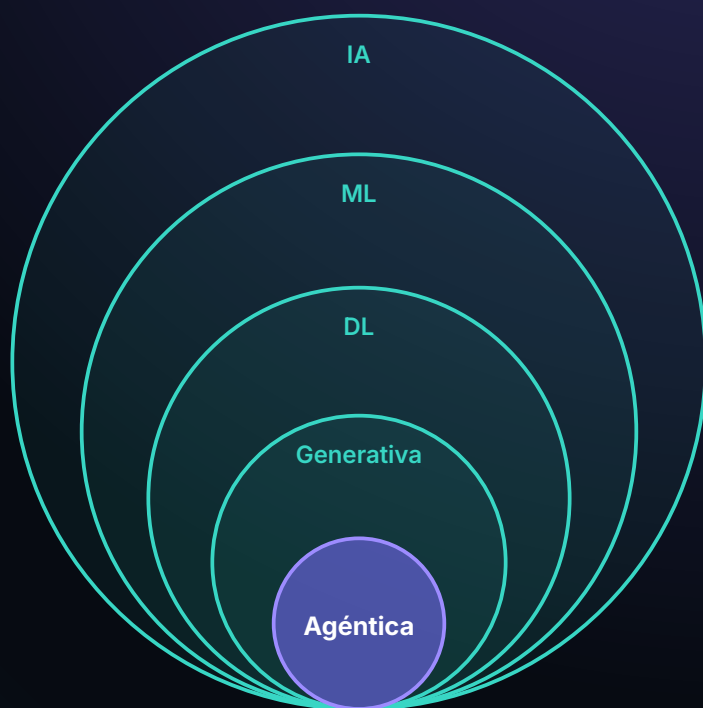




FUNDAMENTOS DE IA

La IA, explicada para decidir mejor

El mapa de la IA, las cuatro ingenierías, qué IA elegir, ciberseguridad y 12 conceptos clave. Sin jerga y sin humo.

01 · EL MAPA DE LA IA

Una dentro de otra



- 1956** **Inteligencia artificial**
"¿Puede una máquina hacerlo?"
- 1997** **Machine Learning**
"¿Qué va a pasar?"
- 2012** **Deep Learning**
"¿Qué hay aquí?"
- 2022** **IA generativa**
"¿Qué escribo o creo?"
- 2025** **IA agéntica**
"¿Qué hago ahora?"

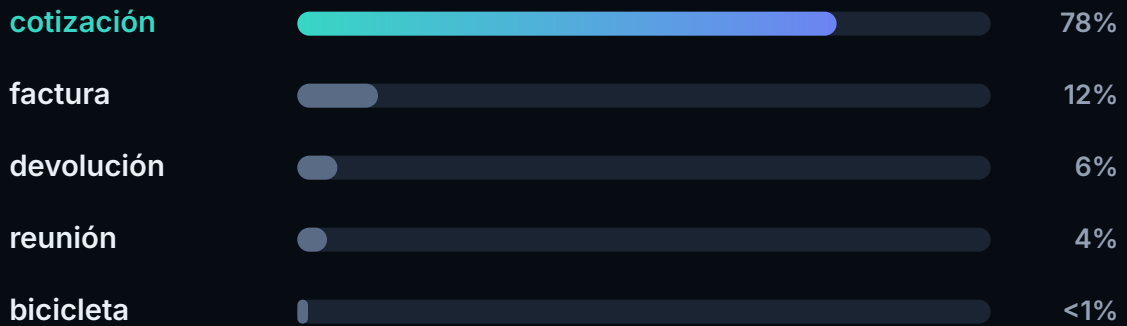
Cada capa se apoya en la anterior. La agéntica usa un modelo generativo como cerebro y le suma herramientas, memoria y un objetivo: no responde y se detiene, trabaja hasta terminar.



02 · CÓMO PIENSA UN MODELO

No busca respuestas: predice la siguiente palabra

El cliente pidió una ____



Probabilidades ilustrativas. El modelo elige entre opciones probables: no sabe si acierta, sabe qué es plausible.

Por eso escribe tan bien

Aprendió de cómo escribimos millones de personas.

Por eso a veces inventa

Plausible no es lo mismo que cierto, y lo dice con la misma seguridad.

Por eso no conoce tu empresa

Sabe de todo en general y nada de lo tuyo, salvo que se lo des.

03 · LAS CUATRO INGENIERÍAS

Prompt, context, loop y graph: cuatro zooms del mismo trabajo

Graph engineering

Un sistema de agentes · ¿El trabajo fluye bien entre todas las piezas?

Loop engineering

Un agente trabajando · ¿Sabe cuándo terminó, cuándo se equivocó y cuándo debe preguntar?

Context engineering

Todo lo que el modelo ve · ¿Tiene a la vista lo que necesita, y nada que lo confunda?

Prompt engineering

Un mensaje · ¿Le pedí bien lo que necesito?

Rol

Eres analista de crédito.

Tarea

Resume este estado financiero en cinco puntos.

Para quién

Un comité, en lenguaje simple.

Formato

Viñetas, y marca cualquier riesgo.

03 · LAS CUATRO INGENIERÍAS

Qué diseñas en cada una

Prompt engineering

Ingeniería de la instrucción

Es como: La instrucción que le das a un colaborador nuevo.

Cómo pides: rol, tarea, contexto, formato y un ejemplo de lo que esperas.

Error típico: Creer que existe una frase mágica. Un buen prompt no compensa información que el modelo no tiene.

Context engineering

Ingeniería del contexto

Es como: El expediente que le entregas junto con la instrucción.

Qué información entra en la ventana del modelo en cada momento: instrucciones, documentos, historial, datos y herramientas disponibles. Y qué se queda afuera.

Error típico: Meter todo "por si acaso". Demasiado contexto cuesta más, es más lento y distrae al modelo.

Loop engineering

Ingeniería del ciclo

Es como: El método de trabajo: hacer, revisar, corregir y entregar.

El ciclo del agente: cómo planifica, qué herramientas usa, cómo verifica su propio resultado, cuándo se detiene y cuándo le pasa la decisión a una persona.

Error típico: Un ciclo sin condición de salida ni presupuesto: el agente gira, gasta y no entrega.

Graph engineering

Ingeniería del flujo

Es como: El organigrama y el flujo de procesos de un equipo.

El mapa entre varios agentes, herramientas y personas: quién hace qué, en qué orden, qué información pasa de uno a otro y qué ocurre si un paso falla.

Error típico: Diez agentes donde bastaba uno. Cada pieza nueva es un punto más que puede fallar.

04 · QUÉ IA ELEGIR

¿ChatGPT, Gemini, Claude o Grok? Depende de para qué

	ChatGPT	Gemini	Claude	Grok
Uso diario, de todo un poco				
Redactar informes y propuestas				
Analizar contratos y documentos largos				
Programar y automatizar				
Trabajar dentro de Gmail, Docs y Drive				
Investigar en la web con fuentes				
Tendencias y redes en tiempo real				
Crear imágenes				
Video, audio y YouTube				
Conversar por voz				

de lo mejor bien sirve, pero hay mejores

Lectura de Balexus, no un benchmark. Revisada en octubre de 2026.

04 · QUÉ IA ELEGIR

El carácter de cada una

**ChatGPT**

OpenAI

El todoterreno

La app con más funciones en un solo lugar: voz, imágenes, búsqueda, investigación profunda, memoria y asistentes a medida.

Ojo: En la cuenta personal, tus chats pueden usarse para entrenar salvo que lo desactives.

**Gemini**

Google

El que vive en tu Google

Integrado en Gmail, Docs y Drive; lee documentos y videos muy largos, y se apoya en la búsqueda de Google.

Ojo: Rinde más si tu empresa ya trabaja en Google Workspace.

**Claude**

Anthropic

El redactor y programador

Escritura con buen criterio y tono, análisis cuidadoso de documentos largos, código y agentes que siguen instrucciones complejas.

Ojo: No genera imágenes ni video.

**Grok**

xAI

El que lee la conversación en vivo

Acceso en tiempo real a lo que se publica en X, tono directo y generación de imágenes.

Ojo: Tiene menos filtros que los otros: revisa la política de tu empresa antes de usarlo con clientes.

Para una empresa, importa más el plan que la marca.

En cuentas personales, lo que escribes puede usarse para entrenar salvo que lo desactives. En planes empresariales y por API, los cuatro ofrecen no hacerlo.

05 · IA Y CIBERSEGURIDAD

La misma herramienta, en dos manos

DEL LADO DEL ATACANTE

Phishing sin errores

Correos personalizados, en perfecto español y con datos reales de tu empresa. Ya no se delatan por la ortografía.

Voz y video falsos

Bastan unos segundos de audio para clonar una voz. El "gerente" que llama pidiendo una transferencia urgente puede no serlo.

Ataques más rápidos

La IA ayuda a encontrar vulnerabilidades y escribir código malicioso en menos tiempo y con menos conocimiento.

Instrucciones escondidas

Texto oculto en un correo, una web o un PDF que intenta darle órdenes al agente que lo lee.

DEL LADO DEL DEFENSOR

Detecta lo anormal

Aprende cómo se comporta tu red y tus usuarios, y avisa cuando algo se sale del patrón.

Ordena las alertas

Un centro de seguridad recibe miles al día. La IA agrupa, prioriza y resume para que el analista mire lo importante.

Revisa lo sospechoso

Analiza correos, enlaces y archivos antes de que alguien haga clic.

Responde antes

Aísla un equipo o bloquea una cuenta en segundos, con una persona aprobando lo grave.

El riesgo más común no es un hacker: es alguien del equipo pegando un contrato en una cuenta gratuita.

05 · IA Y CIBERSEGURIDAD

Ocho reglas para usar IA sin abrir la puerta

Inyección de instrucciones

Texto oculto en un correo, una web o un PDF que intenta darle órdenes al agente que lo lee. La regla: lo que viene de afuera es dato, nunca orden.

- ✓ Nadie pega datos de clientes, contratos o planillas en cuentas personales de IA.
- ✓ Hay una lista de herramientas de IA aprobadas, y se sabe cuáles no.
- ✓ Pagos y cambios de cuenta se confirman por un segundo canal, aunque la voz suene idéntica.
- ✓ Cada agente tiene solo los permisos que su tarea necesita.
- ✓ Toda acción irreversible —pagar, borrar, enviar afuera— la aprueba una persona.
- ✓ Lo que la IA lee de afuera (correos, webs, PDF) se trata como no confiable.
- ✓ Queda registro de qué hizo cada agente y por qué.
- ✓ El equipo sabe reconocer un deepfake y un phishing hecho con IA.

06 · LO QUE HACE MAL

Falla de tres maneras conocidas. Cada una tiene antídoto

FALLA**Inventa con seguridad**

Cuando no sabe, no calla: completa con algo plausible. Se llama alucinación y suena tan convincente como la verdad.

**ANTÍDOTO****Que cite y se verifique**

Responder solo desde fuentes consultadas, mostrando de dónde salió cada dato, y revisión humana donde importa.

FALLA**No sabe lo de ayer**

Aprendió hasta cierta fecha. Lo posterior no existe para él, tampoco lo que pasó en tu empresa esta mañana.

**ANTÍDOTO****Darle acceso, no memoria**

Búsqueda sobre tus documentos y herramientas que consultan tus sistemas en el momento de responder.

FALLA**No ve tus datos**

Sabe de todo en general y nada de ti en particular. Tus precios, tus clientes y tus reglas le son ajenos.

**ANTÍDOTO****Ordenar los datos primero**

Integrados, modelados y con calidad. Sobre datos desordenados, la IA amplifica el desorden.

Si alguien te ofrece IA sin mencionar esto, desconfía.

07 · GLOSARIO ESENCIAL

12 conceptos que vas a escuchar

LLM

Modelo de lenguaje grande: el motor detrás de ChatGPT, Gemini, Claude o Grok.

Token

El trozo de texto con el que trabaja el modelo: una palabra corta o parte de una larga.

Ventana de contexto

Todo lo que el modelo puede tener a la vista a la vez: tu mensaje, el historial y los documentos.

Alucinación

Una respuesta falsa dicha con total seguridad.

RAG

Buscar primero en tus documentos y responder con lo encontrado, citando.

Embeddings

Convertir textos en coordenadas numéricas, de modo que lo parecido quede cerca.

Fine-tuning

Reentrenar un modelo con tus ejemplos para que adopte un estilo o una tarea.

Temperatura

Cuánto se arriesga el modelo al elegir la siguiente palabra.

Multimodal

Que entiende o produce más que texto: imágenes, audio, video.

MCP

Model Context Protocol: un estándar abierto para conectar la IA a tus sistemas.

Guardrails

Barreras que limitan lo que la IA puede decir o hacer.

Humano en el ciclo

Una persona revisa o aprueba en los puntos donde un error cuesta caro.

08 · POR DÓNDE EMPEZAR

El orden importa más que la herramienta

1

Elige un dolor concreto

Medible en horas o en soles. "Implementar IA" no es un objetivo; "dejar de perder cuatro horas a la semana cuadrando inventario" sí.

2

Mira tus datos

¿Existen, están completos, cuadran? Si no, ese es el proyecto, no la IA.

3

Prueba pequeño

Un caso, unas semanas, una métrica. Si no mejora nada medible, no escales: cambia.

4

Prepara a las personas

La herramienta llega en semanas; el hábito toma meses. Sin esto, lo que instalaste no se abre.

LOS TRES ERRORES DE SIEMPRE

- ✗ Empezar por la herramienta y buscarle un problema después.
- ✗ Saltarse el orden de los datos porque "eso lo vemos luego".
- ✗ Comprar licencias para todos sin que nadie sepa para qué.

SIGUIENTE PASO

Ya sabes de qué se trata. Ahora hazlo con tu caso.

AcademIA de Balexus: dos horas en vivo, grupos de hasta diez personas, y sales con algo tuyo funcionando.

balexus.com/academia

Guarda este carrusel y compártelo con tu equipo. La versión interactiva, con la demo de temperatura, el selector de IA y el autodiagnóstico de seguridad, está en balexus.com/fundamentos