AI Congress Barcelona

20 - 21 - 22 OCT 2026

Auditori L'illa

Un esdeveniment de:

CIDAI Centre of Innovation for Data tech and Artificial Intelligence

Organitzat per:

eurecat

Alineat amb l'Estratègia Catalunya IA 2030:

Generalitat de Catalunya

Segueix-nos a:

#AICongressBCN

aicongress.barcelona

Patrocinadors OR:

CaixaBank TECH

conversia compliance is our business

forvis mazars & infini DIGITAL EFFICIENCY

orange Empresas

raona coding corporate futures

softeng Maximize the cloud. Securely.

Patrocinadors PLATA:

apdcat Autoritat Catalana de Protecció de Dades

LABORAL kutxa

Col·laboradors:

Barcelona

BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación

CVC Centre de Visió per Computador

i2cat

UPC Universitat Politècnica de Catalunya BarcelonaTech

IDEAI Intelligent Data Science and Artificial Intelligence Research Center

AI Congress Barcelona

Un esdeveniment de: CIDAI Centre of Innovation for Data tech and Artificial Intelligence

Organitzat per: eurecat

Alineat amb l'Estratègia Catalunya IA 2030: Generalitat de Catalunya

20 - 21 - 22 OCT 2026

#AICongressBCN

aicongress.barcelona

PONÈNCIA:

QUI GOVERNA ELS AGENTS? MCP, ARQUITECTURES MULTIAGENT I RISCOS DE CONTROL



Víctor Garcia
Responsable d'IA
Conversia



Laura Aparicio
Consultora Jurídica Senior
Conversia



Presenta:

Mireya Saludes
Responsable de desenvolupament de negoci i d'ecossistema
CIDAI

Patrocinadors OR: CaixaBank TECH · conversia compliance is our business · forvis mazars & wfini DIGITAL EFFICIENCY · orange Empresas · raona coding corporate futures · softeng Maximize the cloud. Securely.

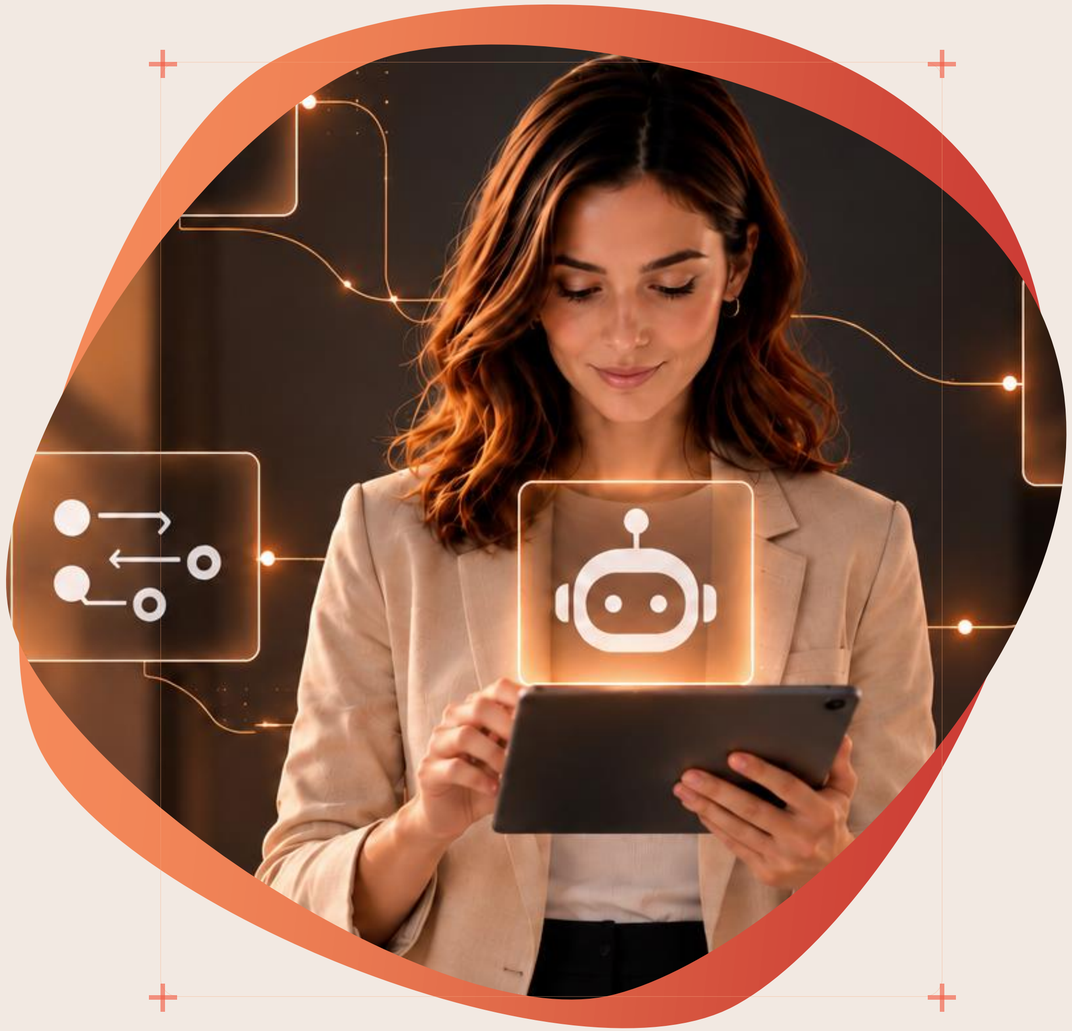
Patrocinadors PLATA: apdcat Autoritat Catalana de Protecció de Dades · LABORAL kutxa

conversia

compliance is our business

¿Quién gobierna a los agentes?

MCP, arquitecturas multiagente y riesgos de control



SOMOS EXPERIENCIA
SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Recorrido de la ponencia

1/ Contexto y tendencias

2/ MCP y Agent2Agent

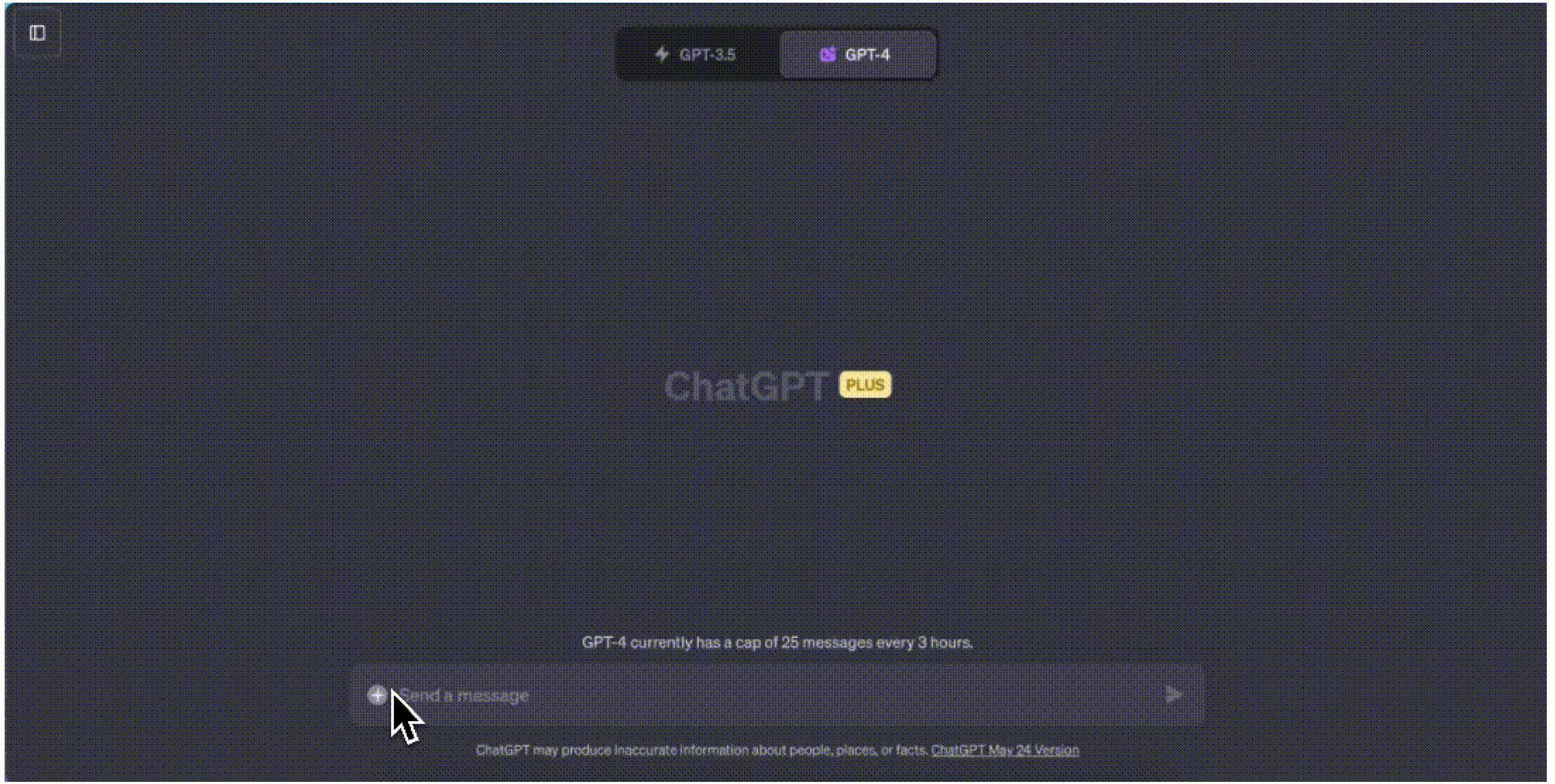
3/ Riesgos y casos de uso malicioso

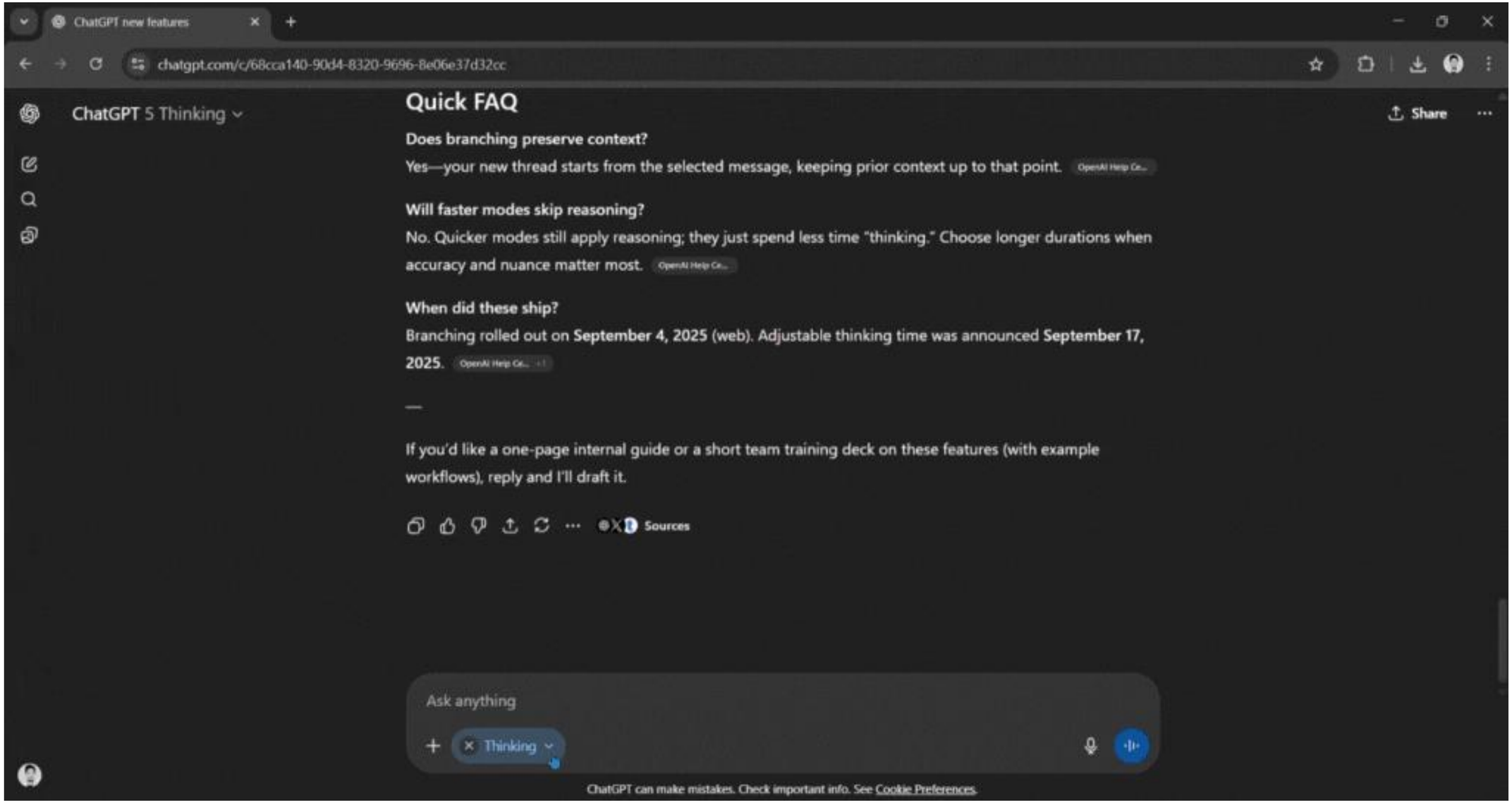
4/ Guía práctica de seguridad

5/ Gobernar la IA

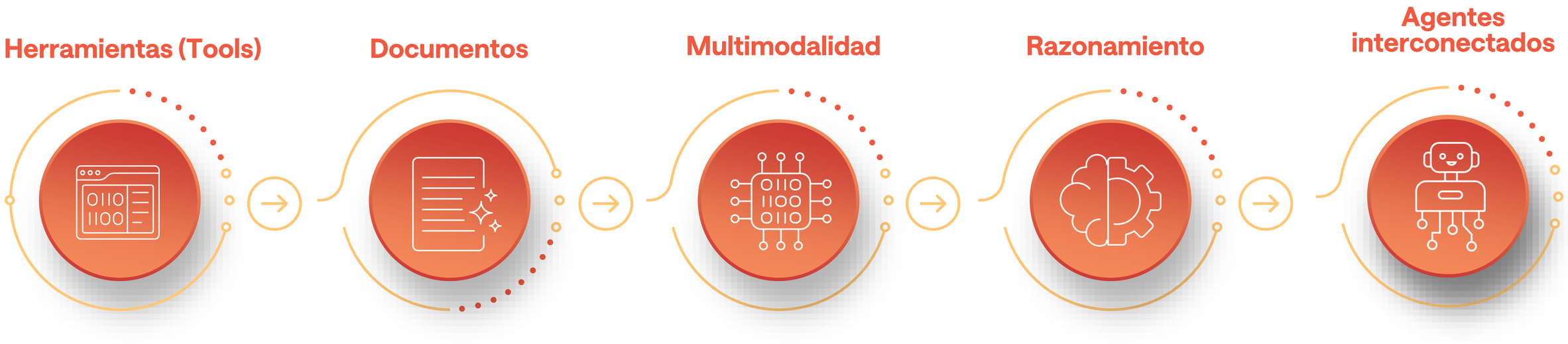
Contexto y tendencias




GPT-3.5
GPT-4
ChatGPT PLUS
GPT-4 currently has a cap of 25 messages every 3 hours.
Send a message
ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 24 Version


ChatGPT new features
chatgpt.com/c/68cca140-90d4-8320-9696-8e06e37d32cc
ChatGPT 5 Thinking
Share
Quick FAQ
Does branching preserve context?
Yes—your new thread starts from the selected message, keeping prior context up to that point.
Will faster modes skip reasoning?
No. Quicker modes still apply reasoning; they just spend less time "thinking." Choose longer durations when accuracy and nuance matter most.
When did these ship?
Branching rolled out on September 4, 2025 (web). Adjustable thinking time was announced September 17, 2025.
—
If you'd like a one-page internal guide or a short team training deck on these features (with example workflows), reply and I'll draft it.
Sources
Ask anything
Thinking
ChatGPT can make mistakes. Check important info. See Cookie Preferences.

De modelos aislados a ecosistemas conectados



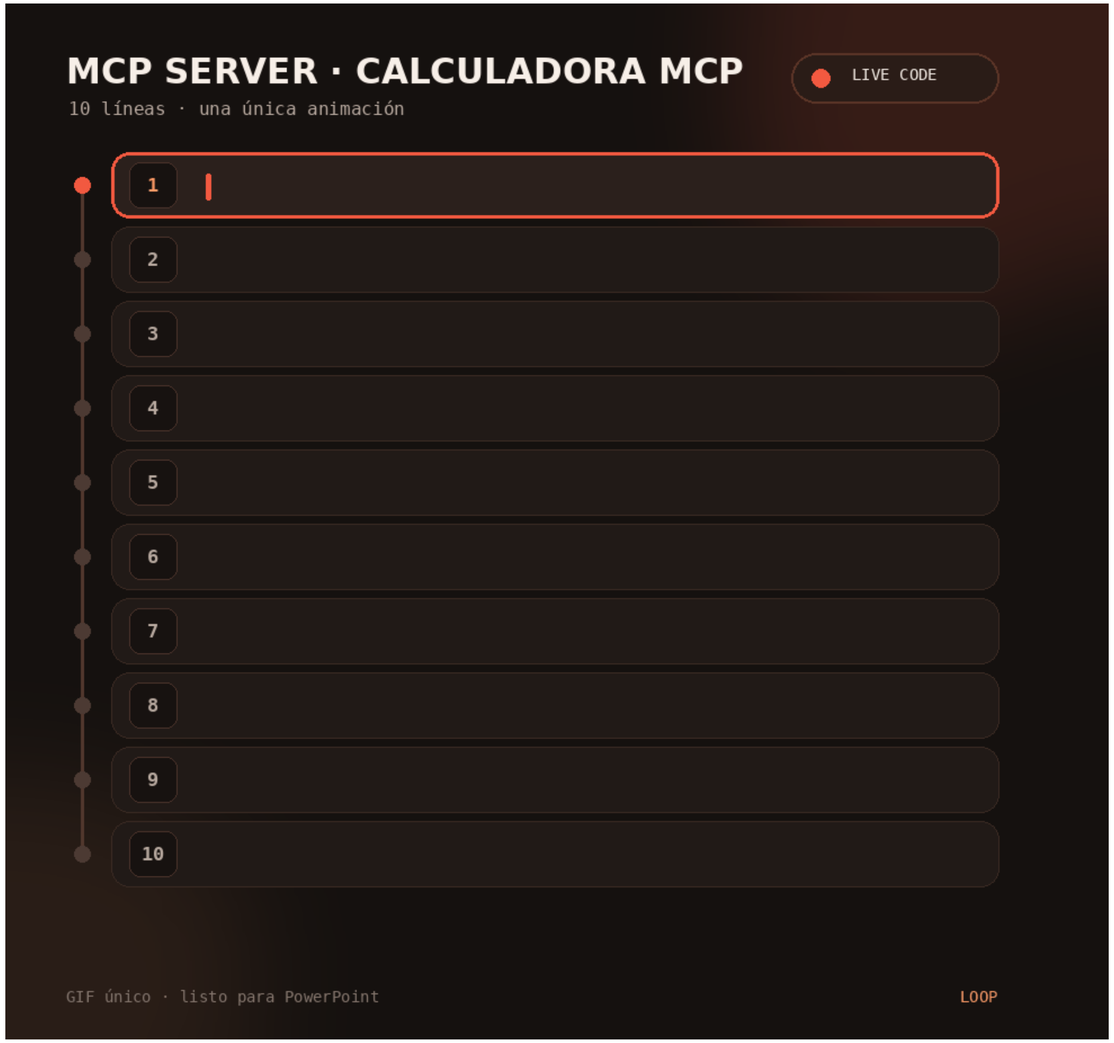
MCP y herramientas



SOMOS EXPERIENCIA
SOMOS REFERENTES

¿Qué es un MCP?

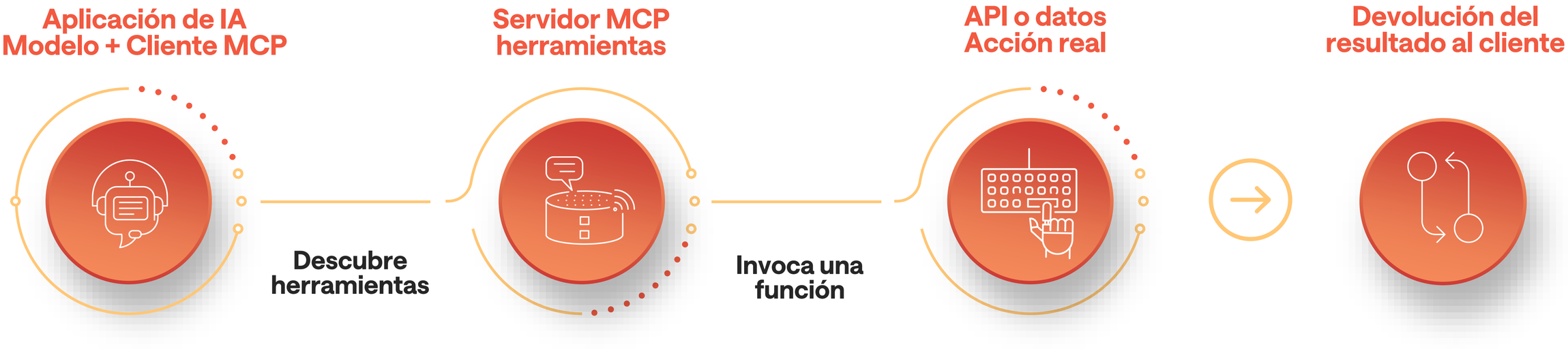
Un protocolo para conectar aplicaciones de IA con herramientas y datos



AI CONGRESS 2026
BARCELONA

MCP
¿Cómo se ejecuta una herramienta?

El modelo propone.
La aplicación y el servicio comprueban los permisos.



Delegar una tarea a otro agente

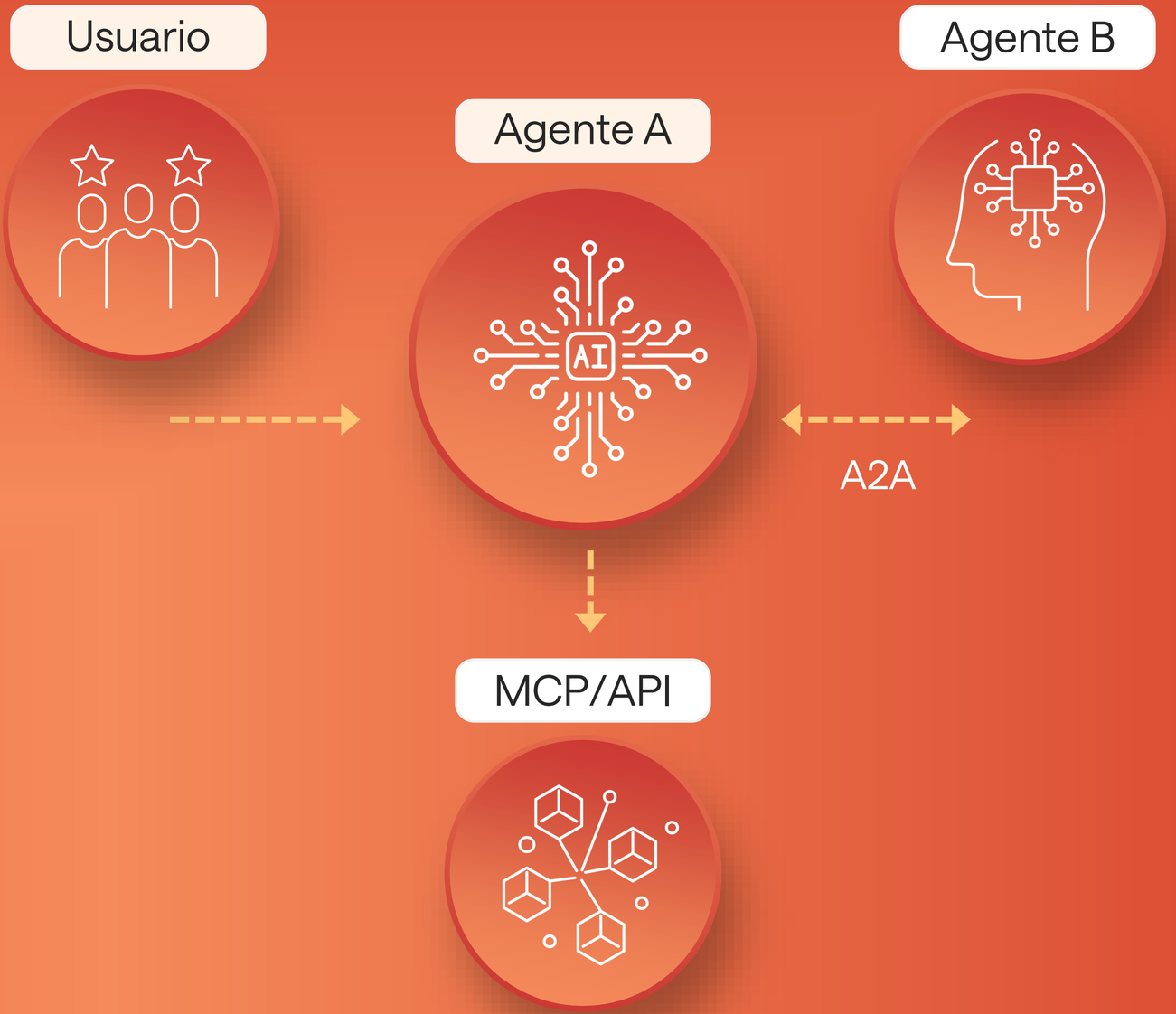
Agent2Agent (A2A)



SOMOS EXPERIENCIA
SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Agentes que colaboran

Un agente coordina especialistas.
Cada servicio valida quién actúa y qué puede hacer.



MCP y A2A
en un ecosistema agéntico



La interfaz visible no revela todos los permisos del sistema.

SOMOS EXPERIENCIA

6 fallos de control

La conexión amplía el alcance del error.



01 Filtración

02 MCP hostil

03 Permisos

04 Delegación

05 Intención

06 Cascada

SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

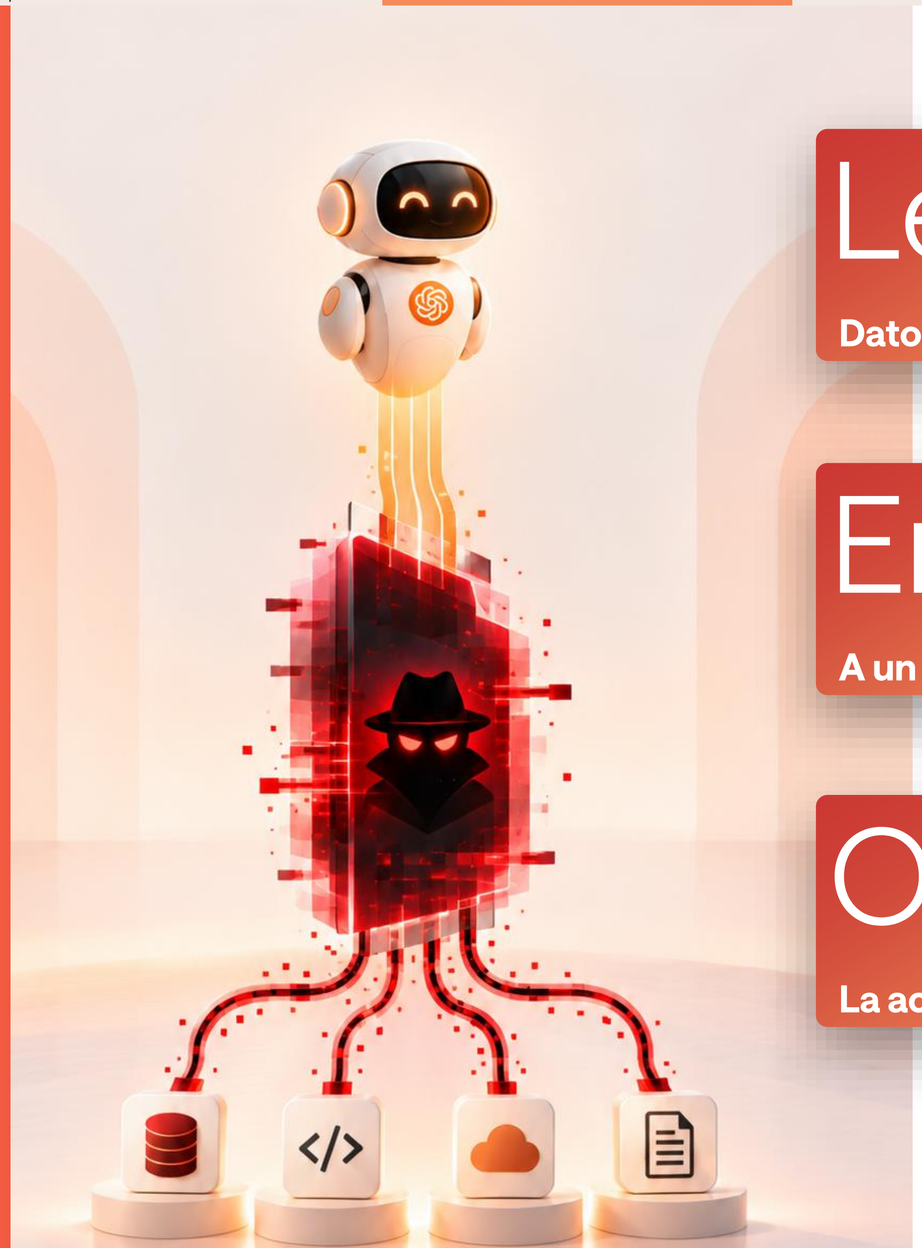
SOMOS EXPERIENCIA

Caso 01 Filtración + MCP malicioso

Un MCP malicioso

- **Promete:**
  Generar prototipos
- **Añade:**
  Una extracción oculta
- **Se contiene con:**
  MCP revisado y red limitada

SOMOS REFERENTES



Lee
Datos no necesarios

Envía
A un destino externo

Oculta
La acción adicional

AI CONGRESS 2026
BARCELONA

SOMOS EXPERIENCIA

Caso 02 Permisos + Intención

Petición

“Mueve la reunión”

- **Mover una sesión de pago.**
- **Conservar asistentes y reservas.**
- **Solo esa sesión.**

Ejecución

- **Interpretación del agente:**
  Error — Confunde mover con cancelar
- **Herramienta elegida:**
  Borrar — Afecta a toda la convocatoria
- **Permisos disponibles:**
  Totales
- **Resultado:**
  Cancelación para todos

Escenario ilustrativo: una sesión de pago termina cancelada para todos

SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Caso 03 Cascada + Permisos

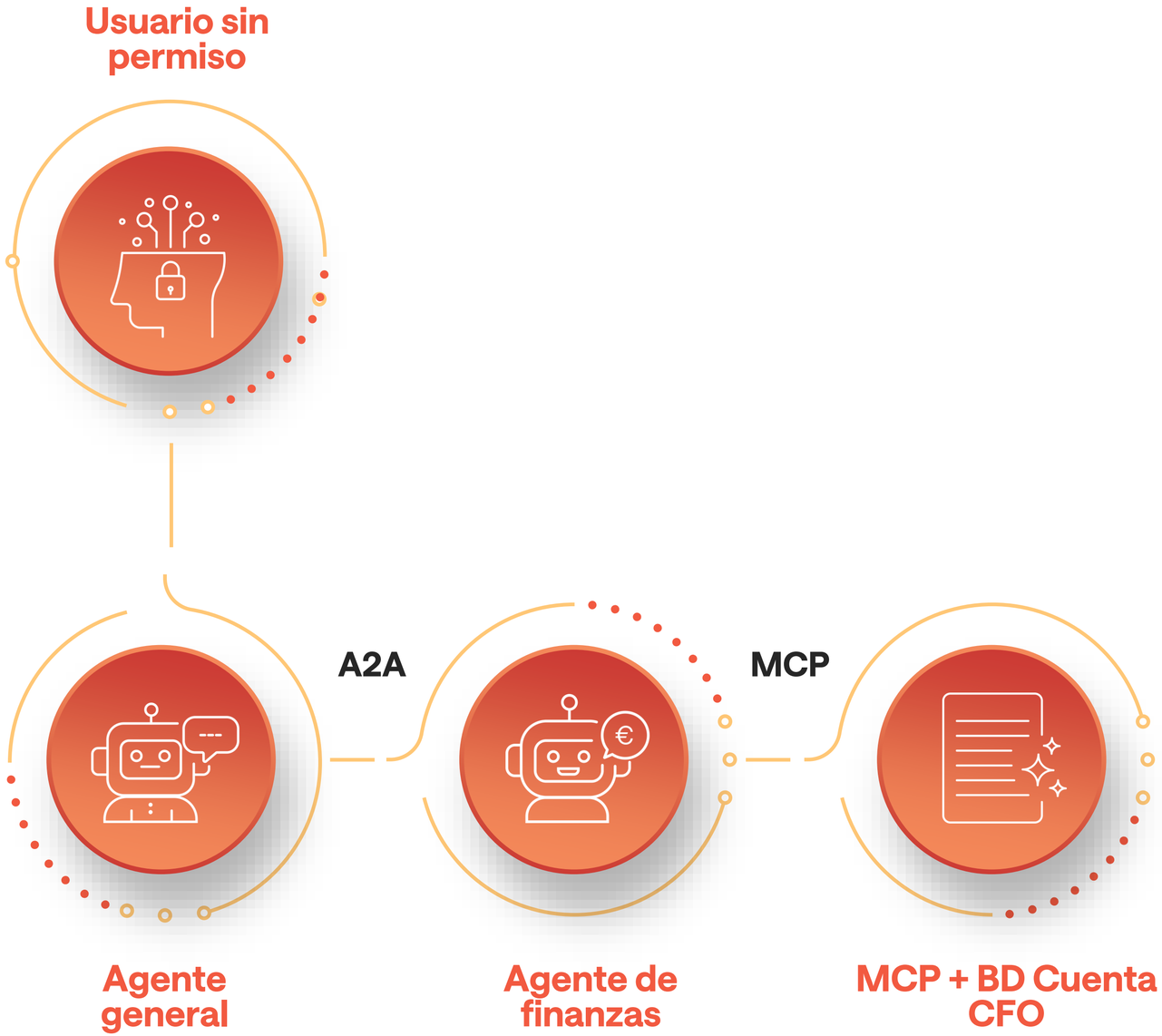
Ataque encadenado: salarios

Fallo:

Finanzas usa privilegios propios sin validar al solicitante original

Control:

Identidad delegada y autorización del dato en cada salto



SOMOS EXPERIENCIA

Caso 04 Cascada + Delegación

Ataque encadenado: borrar una base de datos

- **Control**

  Denegación por defecto y aprobación

  vinculada a la acción exacta



SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Antes de conectar a un agente

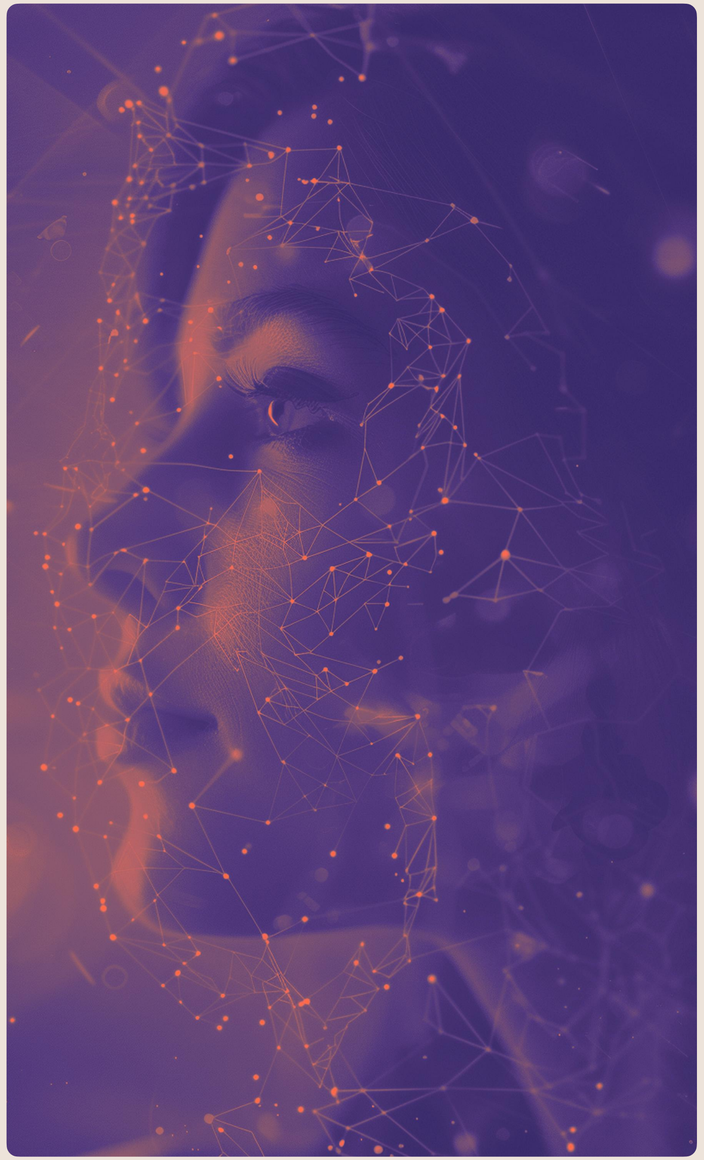
Guía práctica



SOMOS EXPERIENCIA

Antes de usar un agente

Preguntas para cualquier persona, sin necesidad de programar.



01
¿Qué conecto?

02
¿Qué puedo hacer?

03
¿Qué va a enviar?

04
¿Cómo lo paro?

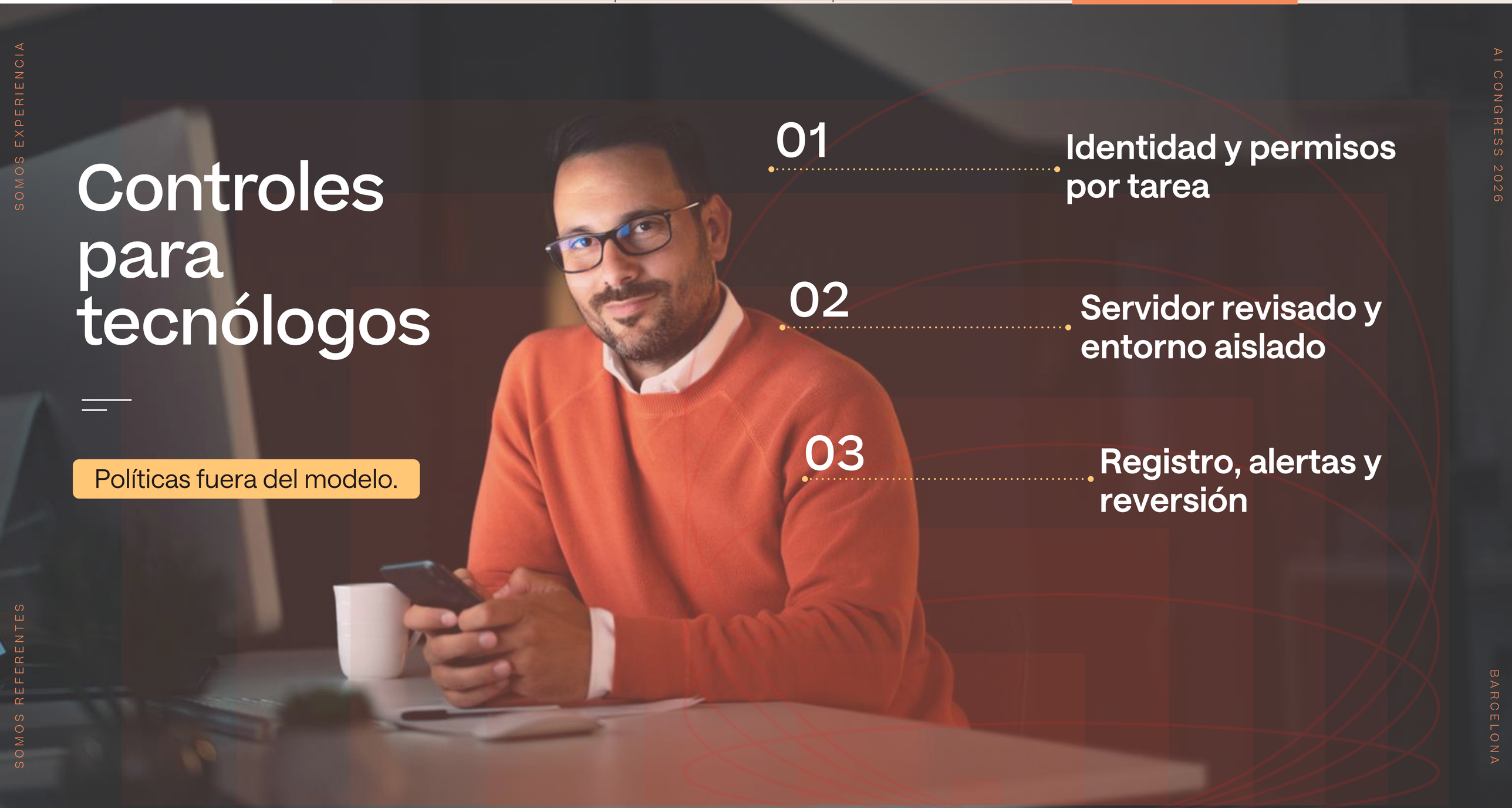
SOMOS REFERENTES

AI CONGRESS 2026
BARCELONA

SOMOS EXPERIENCIA
SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Controles para tecnólogos

Políticas fuera del modelo.



01 Identidad y permisos por tarea

02 Servidor revisado y entorno aislado

03 Registro, alertas y reversión

SOMOS EXPERIENCIA



Pruebas antes del despliegue

01 Usuario sin permiso

02 Documento con una orden maliciosa

03 Acción ambigua

SOMOS REFERENTES
AI CONGRESS 2026
BARCELONA

Gobernar la IA



Cuando la IA empieza a actuar, cambia el perímetro de gobierno

Antes Foco en el modelo



Modelo de IA

Ahora Foco en todo el ecosistema



5 dimensiones para gobernar la IA agéntica

1/ **Identidad y autoridad**
¿Quién actúa y en nombre de quién?

2/ **Autonomía**
¿Hasta dónde puede actuar por sí mismo?

3/ **Datos**
¿Qué puede conocer, utilizar y compartir?

4/ **Delegación**
¿Qué autoridad puede transmitir?

5/ **Trazabilidad y responsabilidad**
¿Podemos reconstruir qué ha ocurrido y quién responde?

1/

Identidad y autoridad

¿Quién actúa y en nombre de quién?

1. **Agent identity**
2. **Least privilege**
3. **Capacidad ≠ Autorización**



SOMOS EXPERIENCIA

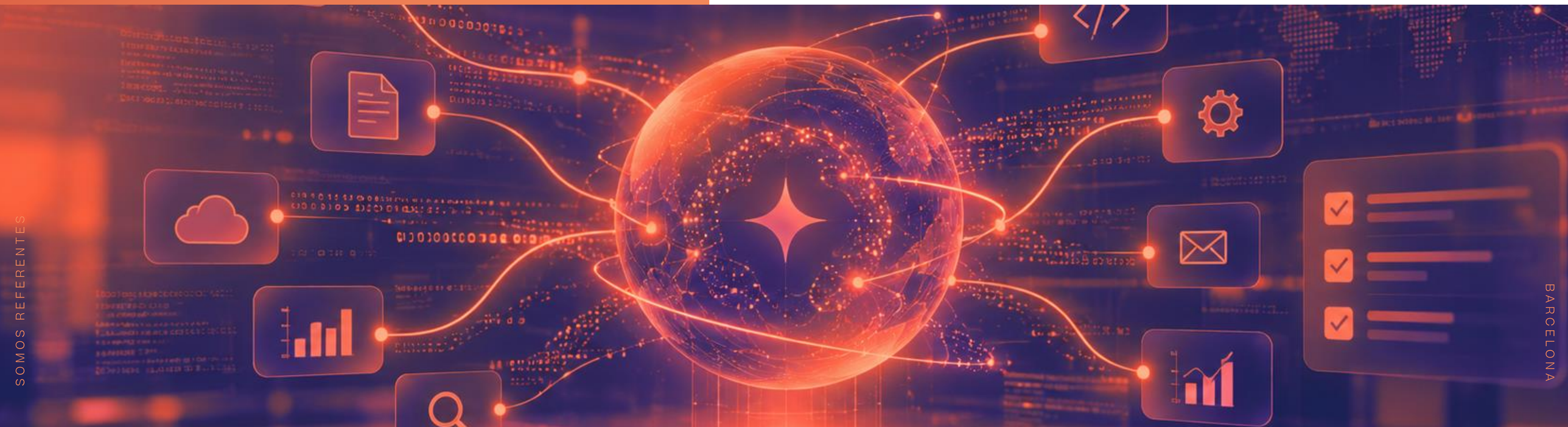
2/

Autonomía

¿Hasta dónde puede actuar por sí mismo?

1. **Diseño Autonomía**
2. **Umbrales de supervisión**
   (Autónomo, HITL, HOTL)
3. **Intervención según riesgo y contexto de uso**

AI CONGRESS 2026



SOMOS REFERENTES
BARCELONA

SOMOS EXPERIENCIA

3/

Datos

¿Qué puede conocer, utilizar y compartir?

1. **Minimización de datos**
2. **Limitación finalidad**
3. **Control de acceso**

AI CONGRESS 2026



SOMOS REFERENTES
BARCELONA

SOMOS EXPERIENCIA

4/

Delegación

¿Qué autoridad puede transmitir?

1. Traslado de la autoridad
2. Alcance
3. Cadena de autoridad

AI CONGRESS 2026



SOMOS REFERENTES
BARCELONA

SOMOS EXPERIENCIA

5/

Trazabilidad y responsabilidad

¿Podemos reconstruir qué ha ocurrido y quién responde?

1. **Reconstrucción de decisiones**
2. **Evidencias auditables**
3. **Atribución de la acción**

AI CONGRESS 2026



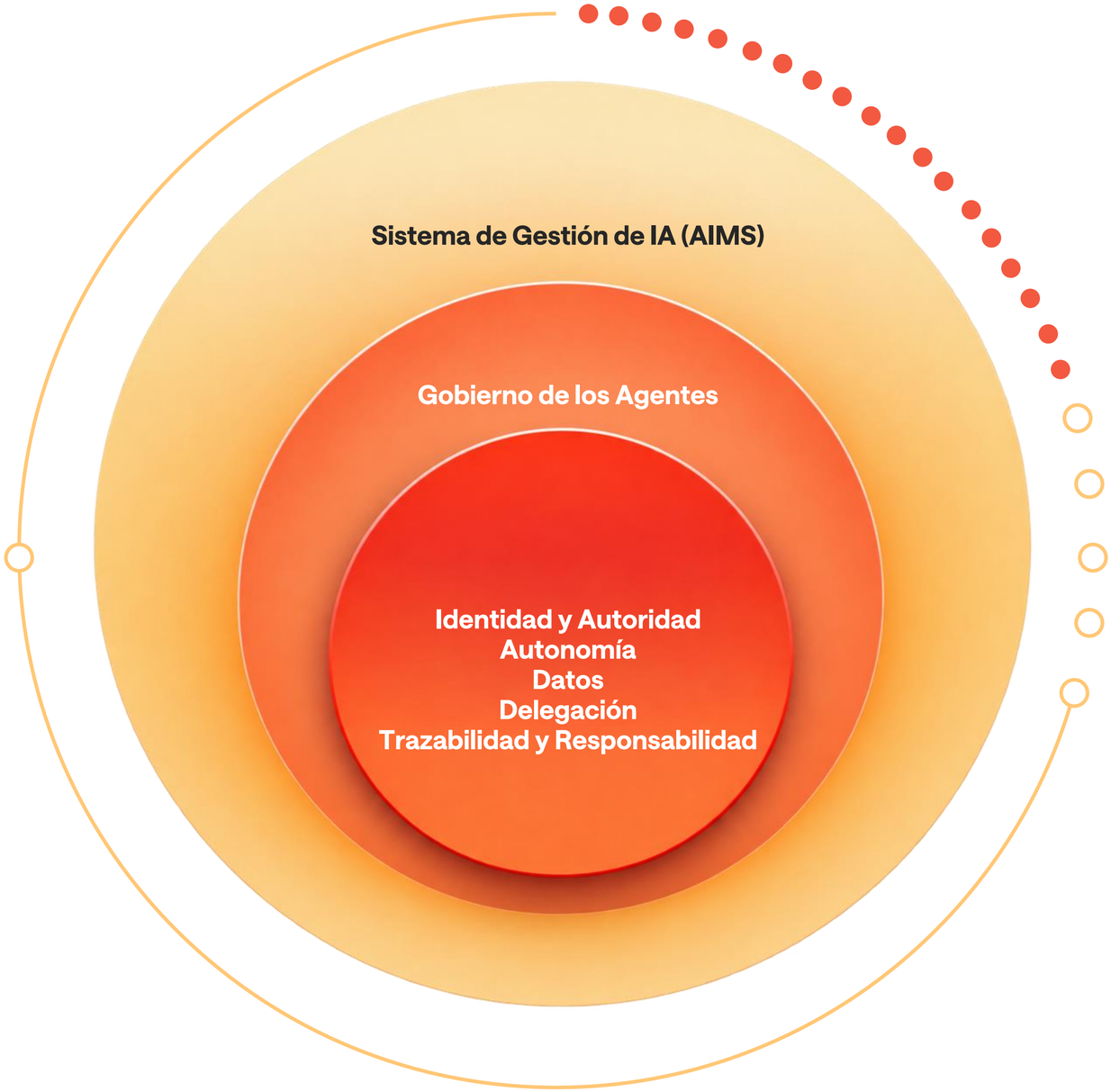
SOMOS REFERENTES
BARCELONA

Gobernanza durante todo el ciclo de vida

No se trata de eliminar la autonomía.
Se trata de gobernarla.



Plan Do Check Act



Muchas gracias

¿Quién puede hacer qué, en nombre de quién?

conversia
compliance is our business



Somos experiencia, somos referentes

AI Congress Barcelona

20 - 21 - 22 OCT 2026

Auditori L'illa

Un esdeveniment de:

CIDAI Centre of Innovation for Data tech and Artificial Intelligence

Organitzat per:

eurecat

Alineat amb l'Estratègia Catalunya IA 2030:

Generalitat de Catalunya

Segueix-nos a:

#AICongressBCN

aicongress.barcelona

Patrocinadors OR:

CaixaBank TECH

conversia compliance is our business

forvis mazars & infini DIGITAL EFFICIENCY

orange Empresas

raona coding corporate futures

softeng Maximize the cloud. Securely.

Patrocinadors PLATA:

apdcat Autoritat Catalana de Protecció de Dades

LABORAL kutxa

Col·laboradors:

Barcelona

BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación

CVC Centre de Visió per Computador

i2cat

UPC Universitat Politècnica de Catalunya BarcelonaTech

IDEAI Intelligent Data Science and Artificial Intelligence Research Center