

Gobernanza de la IA para Ecosistemas Humanware

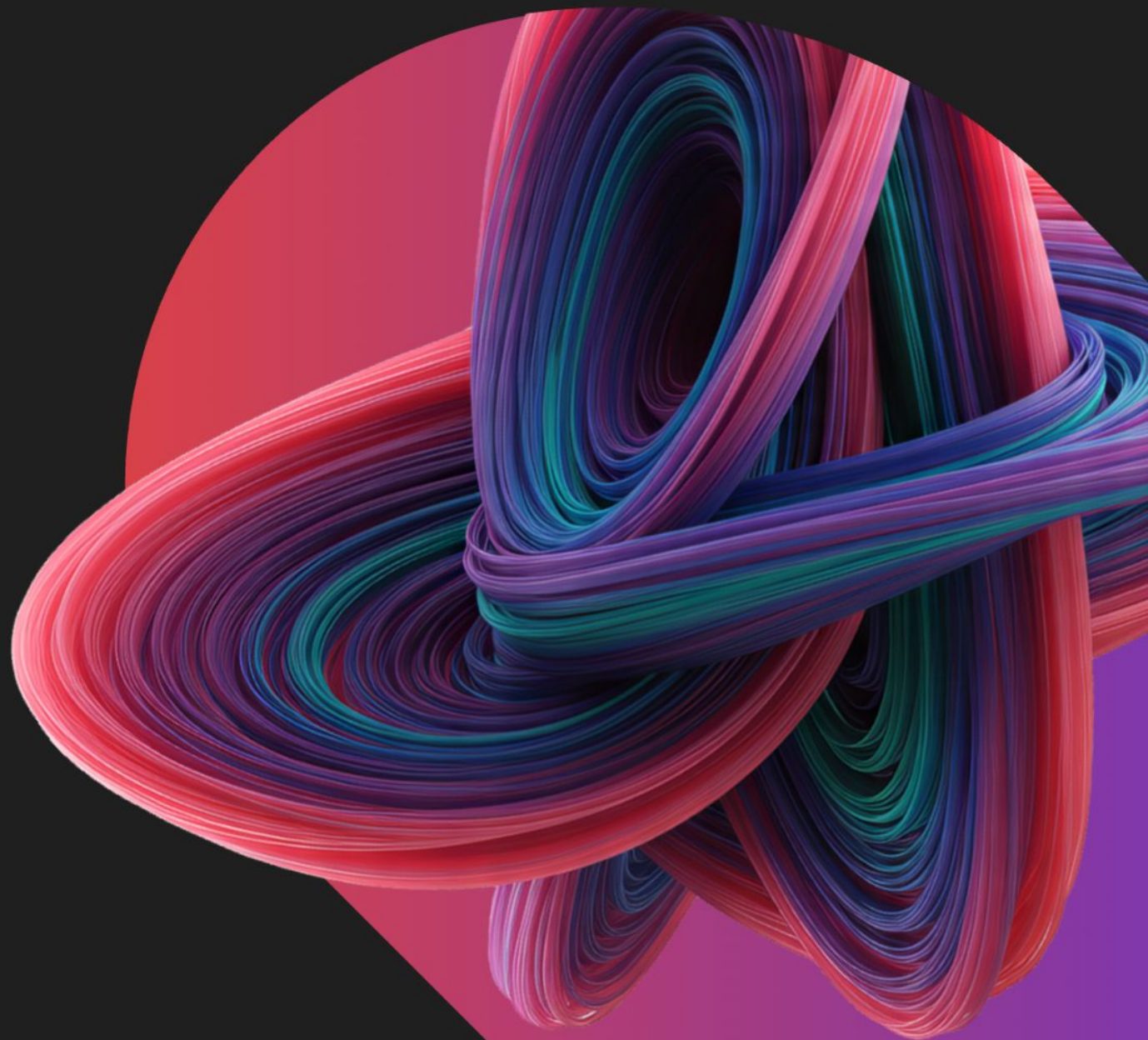
5.0: Marcos, Riesgos y Oportunidades

Cómo ponerle sentido común, barandas y control real a la tecnología en el día a día.

Ing. Federico Piñeyro | XXIV CIITI 2026



Marcos de Gobernanza



Gobernar la IA no es prohibir la innovación, sino **crear las condiciones seguras** para acelerarla



01

Principios y Políticas Claras

Definir qué valores, normativas y límites éticos guían el uso de la IA en la organización



02

Clasificación Basada en Riesgo

Diferenciar tareas de bajo impacto (asistenciales) de procesos críticos (decisiones automatizadas que impactan a personas o al negocio).



03

Rendición de Cuentas

(Accountability) y Semáforos

El humano siempre retiene el timón (Human-in-the-loop o Human-on-the-loop)

Los estándares que marcan el camino

Buenas prácticas globales para gobernar la IA sin reinventar la rueda.



01

NIST AI Risk Management Framework (RMF)

4 Funciones Clave:

Gobernar • Mapear • Medir • Gestionar

El estándar de facto para identificar y mitigar riesgos de IA a nivel empresarial.



02

Enfoque Regulatorio por Niveles de Riesgo

Riesgo Inaceptable

Prohibido.

Alto Riesgo

Supervisión humana estricta, registros y auditorías.

Riesgo Limitado / Mínimo

Transparencia y barandas para operar con agilidad.



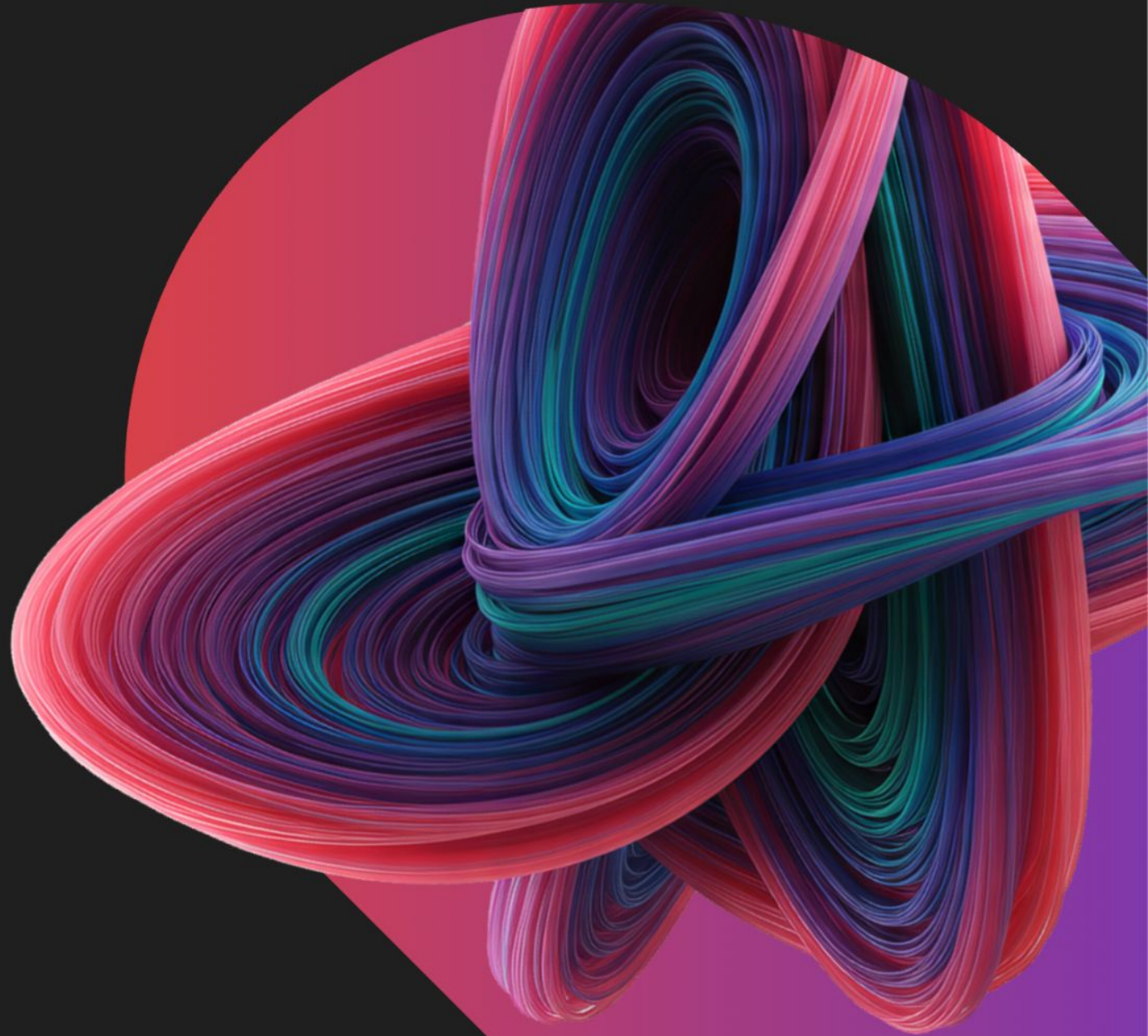
03

El rol de Humanware 5.0

"Las normas no sirven en un cajón"

El marco de gobernanza debe integrarse de forma natural en el flujo de trabajo diario de las personas y los equipos.

Los riesgos



El GPS te sugiere la ruta, el volante lo tenes vos

La Inteligencia Artificial como copiloto, el criterio humano en el control.



La tentación del piloto automático

01

Hoy usamos herramientas de IA para redactar correos, resumir informes o automatizar tareas en segundos.

Es fácil caer en la tentación de cederle todo el control a la máquina.



El sentido común no se delega

02

Si un GPS ultra sofisticado te manda directo a contramano por un puente roto, tu criterio humano frena.

Con la inteligencia artificial pasa exactamente lo mismo:

la tecnología propone, el humano decide.

Los Riesgos: ¿Qué pasa cuando dejamos a la IA suelta?



Alucinaciones seguras

Las IA a veces inventan datos, precios o normas con total seguridad y tono convencido. Si no hay supervisión, un error técnico se convierte en un problema real.



Falta de empatía

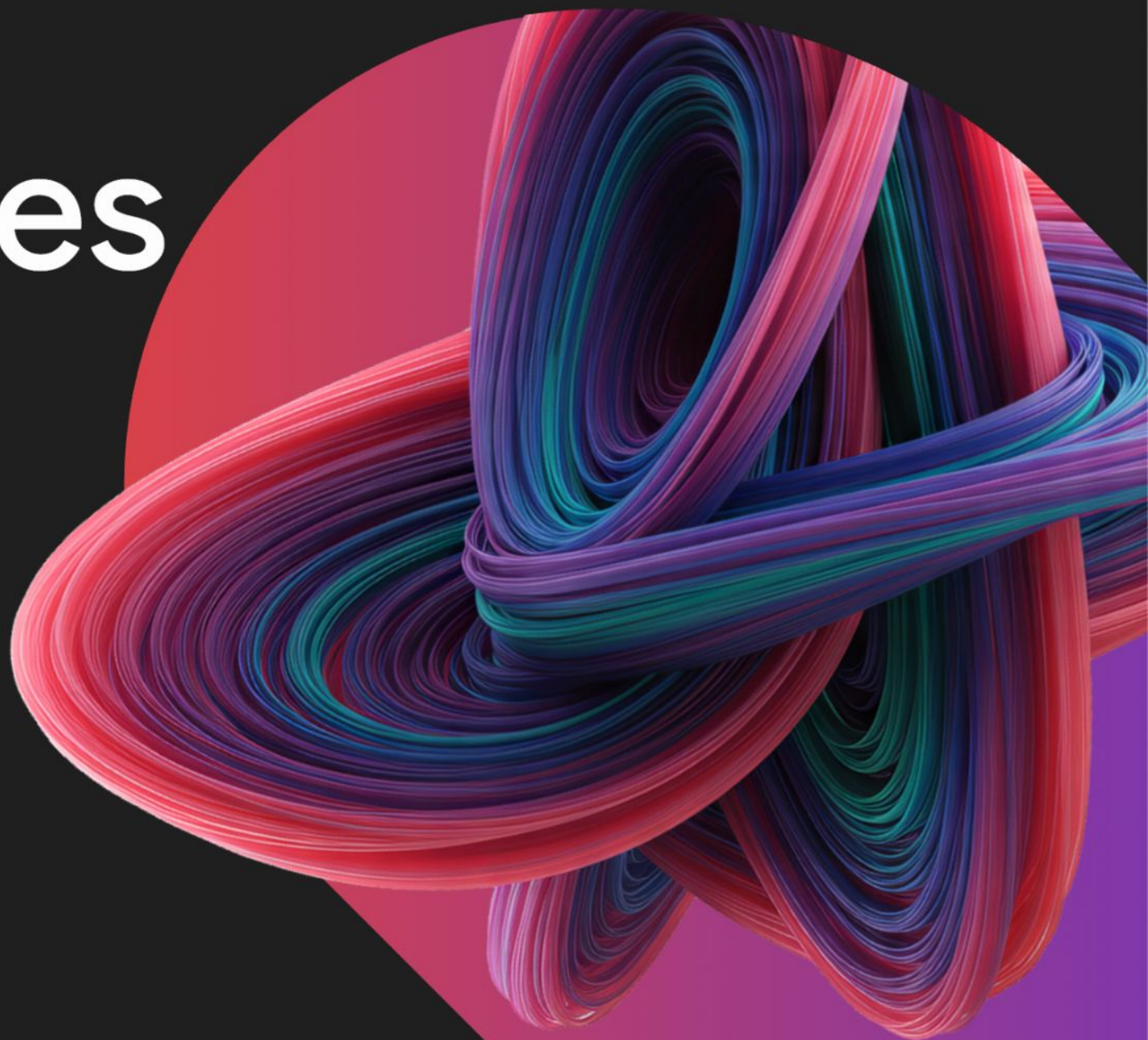
Un sistema automatizado carece de contexto emocional. Responderle de forma fría y robótica a un cliente enojado o a una situación delicada puede destruir la confianza.



Decisiones sin brújula

La máquina procesa probabilidades a velocidad luz, pero no distingue lo que es justo, ético o conveniente para el negocio y la sociedad.

Las oportunidades



Las Oportunidades: El Chef y sus robots ayudantes



Velocidad y trabajo pesado

Imaginá una cocina profesional donde robots veloces cortan verduras, baten y ordenan las bandejas a milisegundos. La IA asume toda la fricción operativa y repetitiva.



El valor está en el criterio humano

El chef (vos) es el único que prueba el plato, ajusta los condimentos y decide si está listo para servir. La IA libera tiempo para focalizarnos en la estrategia, la creatividad y las personas.



La Gobernanza: Barandas claras y semáforos inteligentes



Límites claros de diseño

Construir herramientas que sepan reconocer sus propios límites y avisen claramente cuando no están seguras de una respuesta.



El botón de parada

Siempre debe existir un mecanismo simple para que una persona intervenga, corrija o frene el proceso automático a tiempo.



Responsabilidad final

La máquina puede equivocarse, pero la responsabilidad ética y legal frente al impacto siempre recae sobre el humano.



¿Cómo llevamos el semáforo y las barandas a la ingeniería real?

Un marco de gobernanza no puede ser solo un PDF de políticas: debe ser código ejecutable y arquitectura viva.



01

De la regla abstracta → a las barreras automáticas

(Agent Policy & Model Armor)

Protección en tiempo real contra inyecciones de prompts, fugas de datos y respuestas fuera de política.



02

Del rol humano → a la identidad del agente

(Agent Identity & Access Management)

Cada agente opera con credenciales, permisos acotados y principio de menor privilegio, igual que un empleado o servicio.



03

De la auditoría teórica → a la observabilidad operativa

(Agent Gateway & Observability)

Registro de trazas, costos, decisiones e intervenciones humanas en una consola centralizada.

Gemini Enterprise Agent Platform



01

Desarrollo Veloz

Permite pasar del prototipo a producción a gran velocidad empleando los modelos más avanzados (familia Gemini) y opciones de terceros.



02

Gobernanza y Control

Ofrece un control centralizado para administradores desde la consola de Google Cloud para monitorear **costos**, configurar **accesos** y garantizar que los datos corporativos no se utilicen para entrenar modelos públicos.

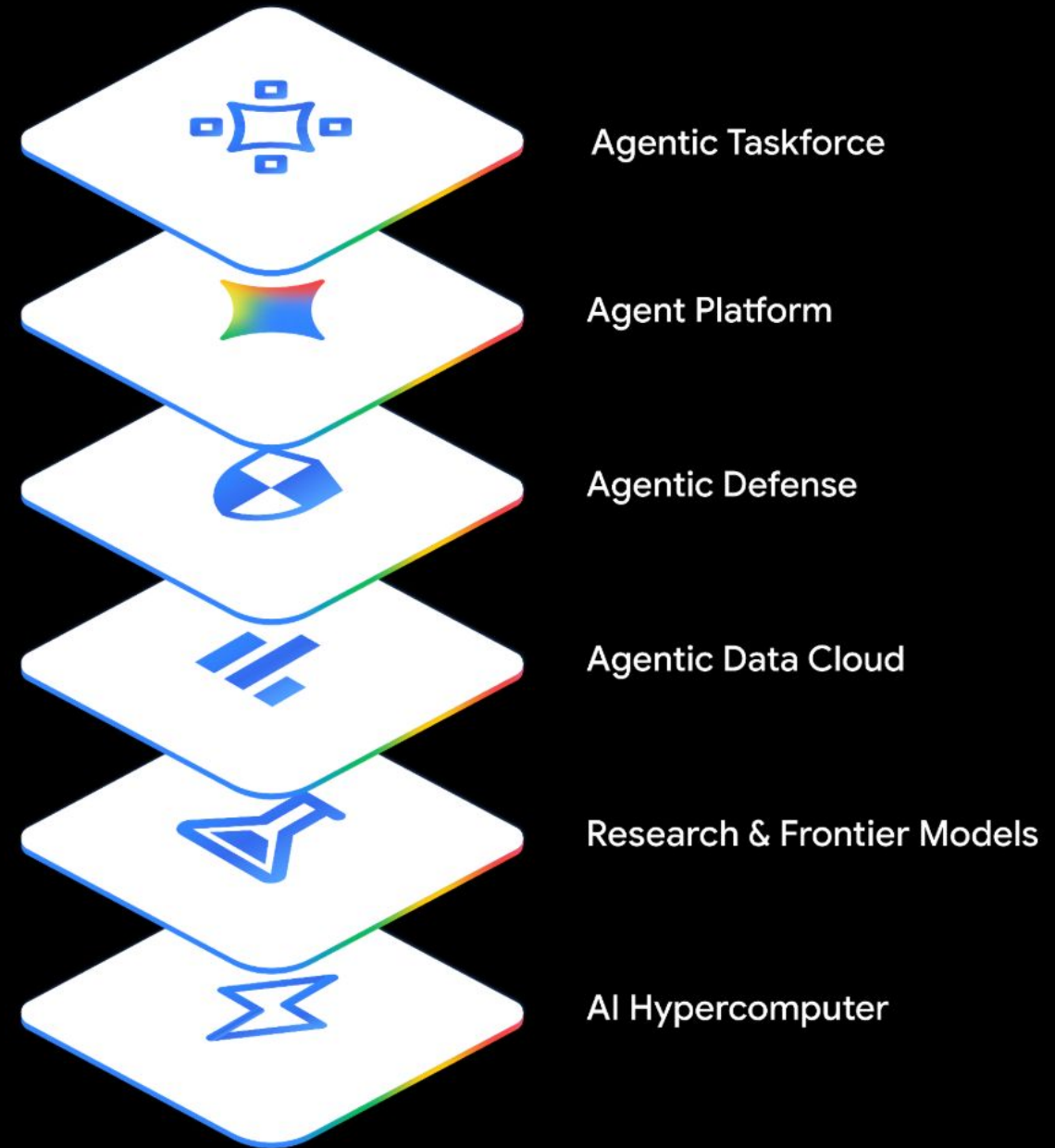


03

Agentic Data Cloud

Actúa como el motor que conecta y "ateriza" (**grounding**) a los agentes con datos empresariales en tiempo real para que actúen con total fidelidad y contexto de negocio.

Google Cloud
ofrece soluciones
propias en toda la
pila de IA.



¿Cómo logran las empresas **resultados de negocio** con agentes de IA?

Calidad

¿Cómo creamos agentes que realmente ofrezcan resultados de alta calidad alineados con nuestras necesidades empresariales?



Integración

¿Cómo permitimos que los empleados de toda la organización integren agentes en su trabajo diario, conectados a sus datos y sistemas?



Confianza

En un mundo con decenas de miles de agentes en funcionamiento que tienen acceso a todos nuestros sistemas y datos, ¿cómo podemos confiar en que todo está gestionado y seguro?



Innovación

¿Cómo nos mantenemos al día con el rápido ritmo de cambio en la IA?



Cómo aborda Gemini Enterprise estos desafíos

Crear (Antigravity)

Capacita a cada empleado para crear agentes de alto impacto en el nivel de abstracción adecuado.



Escala

Herramientas para gestionar agentes a escala en toda su organización con visibilidad y observabilidad profundas.



Gobierno

Gobierno y seguridad mediante seguridad de agentes, gestión de identidades, pasarelas y registros.



Optimiza

Acelera la innovación aprovechando lo mejor de Google y el ecosistema abierto.



✦ Gemini Enterprise Architecture Overview

APPLICATIONS & SOLUTIONS

✦ Gemini Enterprise App

▲ Google Antigravity

✦ Gemini for Customer Experience

🔑 Custom Apps (You / Partners)

✦ Gemini Enterprise Agent Platform



1P, 3P & Open
Models



Model Tuning &
Training



Agent
Frameworks &
APIs



Agent Runtimes &
Sandboxes



Agent
Governance



Policy & Security
Gateways



Advanced Threat
Detection



Observability,
Eval & Sim

AGENTIC CAPABILITIES LIFECYCLE

BUILD

SCALE

GOVERN

OPTIMIZE

POWERED BY THE INTEGRATED STACK FOR AGENTIC AI

⚡ AI Hypercomputer

☁ Agentic Data Cloud

🛡 Agentic Defense



Gemini Enterprise Agent Platform

BUILD

Gemini API & Model Garden

Agent Dev Kit

3P Frameworks

Gemini Models

3P & Open Models

Model Training

Model Inference

Tools, Data & Extensions

Agent Studio

Agent Garden

Skills & MCP

Grounding & RAG

Search & APIs

A2A & A2UI

AP2 & UCP

Marketplace

SCALE

Agent Runtime

Agent Sessions

Agent Sandbox

Agent Memory Bank

GOVERN

Agent Gateway & Armor

Agent Identity & Policy

Agent Registry & Security

Anomaly Detection

Model Armor

Agent Policy

Agent Compliance

Agent Security

OPTIMIZE

Agent Evaluation

Agent Simulation

Agent Observability

Agent Optimizer

Gemini 3.7 Flash: ejemplos de casos de uso

Agentic coding and behavior



DevTools and IT:

Tareas de ingeniería de software con seguimiento del repositorio



SaaS and ops:

Planificación de la verificación y defensa de restricciones



Finance and legal:

Paneles de visualización de consultas sobre múltiples documentos

Knowledge Work



Financial Services:

Análisis de gráficos financieros y archivos PDF de resultados



Retail:

Informes de inventario visual



Software Development:

Reducción del tiempo de revisión manual de especificaciones

Web development



E-commerce:

Creación de una web app con parallax dinámico en poco tiempo



Design to code:

Traduce los diseños de pantalla de Figma a producción.



Financial Services:

Interfaces de usuario personalizadas para informes de clientes

¿Consultas?

XXIV CIITI 2026 — Ing. Federico Piñeyro (Google)

Gracias!

XXIV CIITI 2026 — Ing. Federico Piñeyro (Google)