databricks × Medalla TECHNOLOGY

Databricks Deep Dive: Enterprise-Scale AI Agents

Martes 24 de Marzo | 10:00 – 14:30

UDIT UNIVERSIDAD DE DISEÑO Y TECNOLOGÍA

databricks

Medalla TECHNOLOGY

Databricks FinOps

Controlando nuestros costes

UDIT UNIVERSIDAD DE DISEÑO Y TECNOLOGÍA

Los problemas

Costes no controlados.

Reparto de costes por consumidores.

Ineficiencias en la infraestructura.

Nuestra propuesta

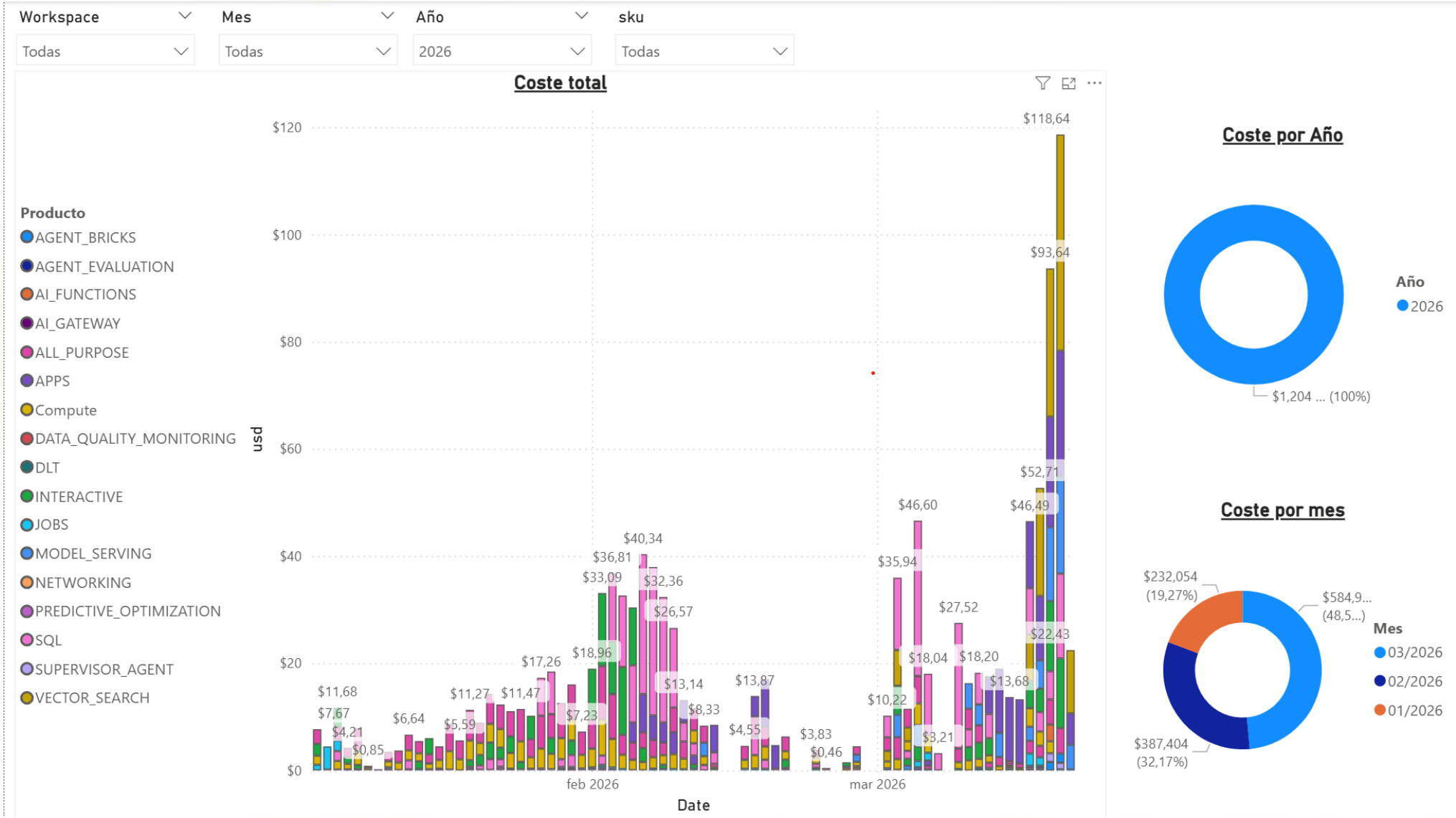
Etiquetado de recursos

Coste global

Análisis del consumo

Visión 360°

Detectamos tendencias e irregularidades de un vistazo

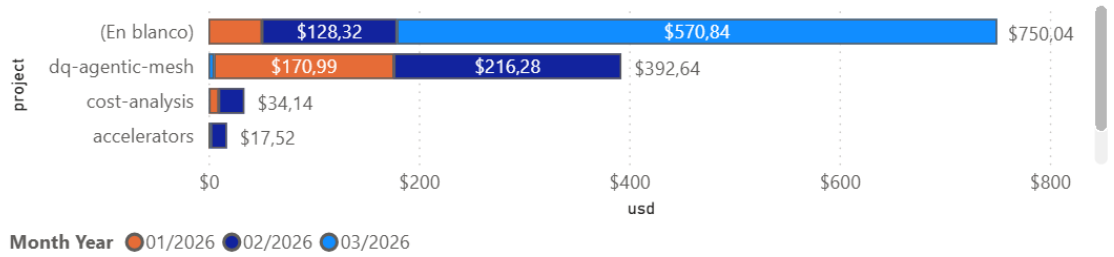


Organización de costes

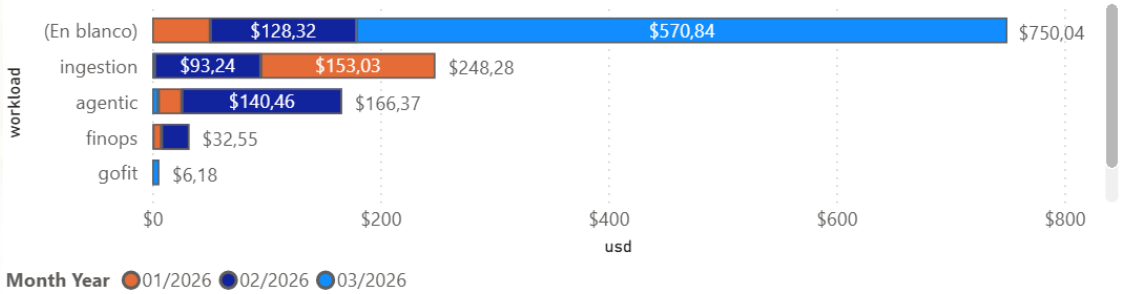
Medalla TECHNOLOGY

Workspace	Mes	Año	env	project	workload
Todas	Todas	2026	Todas	Todas	Todas

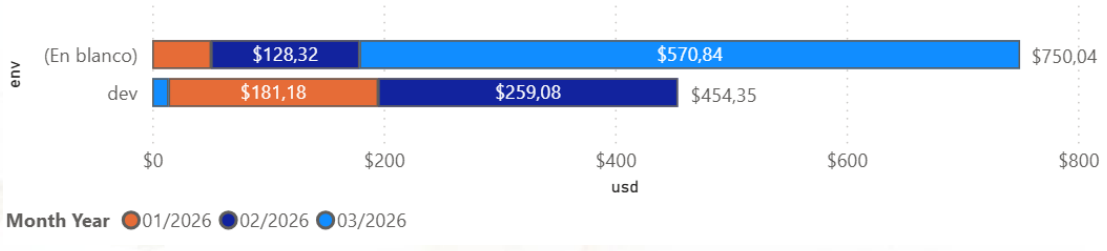
Coste por proyecto



Coste por workload



Coste por entorno



Detalles

env	project	workload	Año	Mes	Día	Coste
			2026	febrero	20	$1,616
dev	cost-analysis	finops	2026	febrero	20	$4,151
dev	dq-agentic-mesh	agentic	2026	febrero	20	$0,244
dev	dq-agentic-mesh	ingestion	2026	febrero	20	$0,321
			2026	febrero	23	$0,454
dev	cost-analysis	finops	2026	febrero	23	$3,378
dev	cost-analysis	finops	2026	febrero	24	$0,398
dev	dq-agentic-mesh	agentic	2026	febrero	24	$0,064
			2026	febrero	26	$0,759
dev	dq-agentic-mesh	ingestion	2026	febrero	26	$0,733
			2026	febrero	27	$1,897
dev	demo	agentic	2026	febrero	27	$2,083
dev	dq-agentic-mesh	agentic	2026	febrero	27	$0,247
dev	dq-agentic-mesh	ingestion	2026	febrero	27	$0,279
			2026	marzo	2	$9,566
dev	demo	agentic	2026	marzo	2	$0,653
			2026	marzo	3	$35,940
			2026	marzo	4	$11,531
			2026	marzo	5	$45,955
dev	dq-agentic-mesh	agentic	2026	marzo	5	$0,647
			2026	marzo	6	$16,753
dev	dq-agentic-mesh	agentic	2026	marzo	6	$1,283
			2026	marzo	7	$3,209
			2026	marzo	9	$26,897
dev	cost-analysis	finops	2026	marzo	9	$0,370
dev	dq-agentic-mesh	agentic	2026	marzo	9	$0,255
			2026	marzo	10	$15,060
Total						**$1.204,388**

Análisis de ejecuciones

Job	Mes	Coste
Jobs Test FinOps	02/2026	$1,258
Total		**$1,258**

Date	Job	Cluster	Recomendación GC	Recomendación CPU	Recomendación Memoria	Recomendación Ejecutores
18/02/2026	Jobs Test FinOps	0218-121721-u9qs25li	Saludable	CPU adecuado	Severo: Aumentar mem...	Subutilización moderada ...
18/02/2026	Jobs Test FinOps	0218-163208-kk3dky2a	Saludable	CPU adecuado	Severo: Aumentar mem...	Utilización aceptable - C...
23/02/2026	Jobs Test FinOps	0223-115711-tykh1qcy	Saludable	CPU adecuado	Crítico: Aumentar mem...	Subutilización moderada ...
23/02/2026	Jobs Test FinOps	0223-150812-edw6td...	Saludable	Subutilizado: Reducir cores	Memoria adecuada	Solo driver - Configuraci...
23/02/2026	Jobs Test FinOps	0223-151252-pjnf5inm	Saludable	Subutilizado: Reducir cores	Memoria adecuada	Utilización óptima - Man...

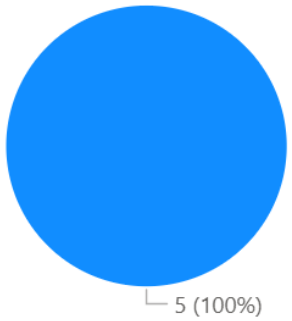
Valores recomendación GC
Saludable

Valores recomendación CPU
Subutilizado: Reducir cores
CPU adecuado

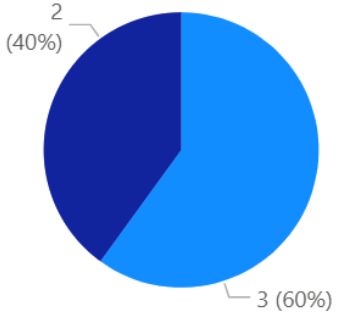
Valores recomendación memoria
Severo: Aumentar memoria
Crítico: Aumentar memoria
Memoria adecuada

Valores recomendación workers
Subutilización moderada - Reducir workers
Utilización aceptable - Considerar reducción moderada
Utilización óptima - Mantener configuración
Solo driver - Configuración adecuada

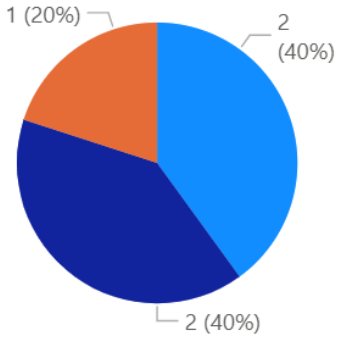
Recomendación GC



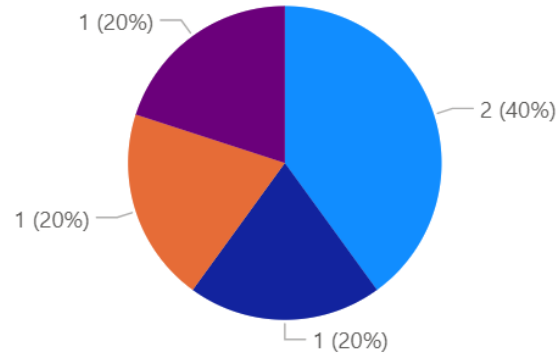
Recomendación CPU



Recomendación Memoria



Recomendación Ejecutores



databricks

Medalla TECHNOLOGY

Estrategia de Datos en la era de la IA Agéntica:

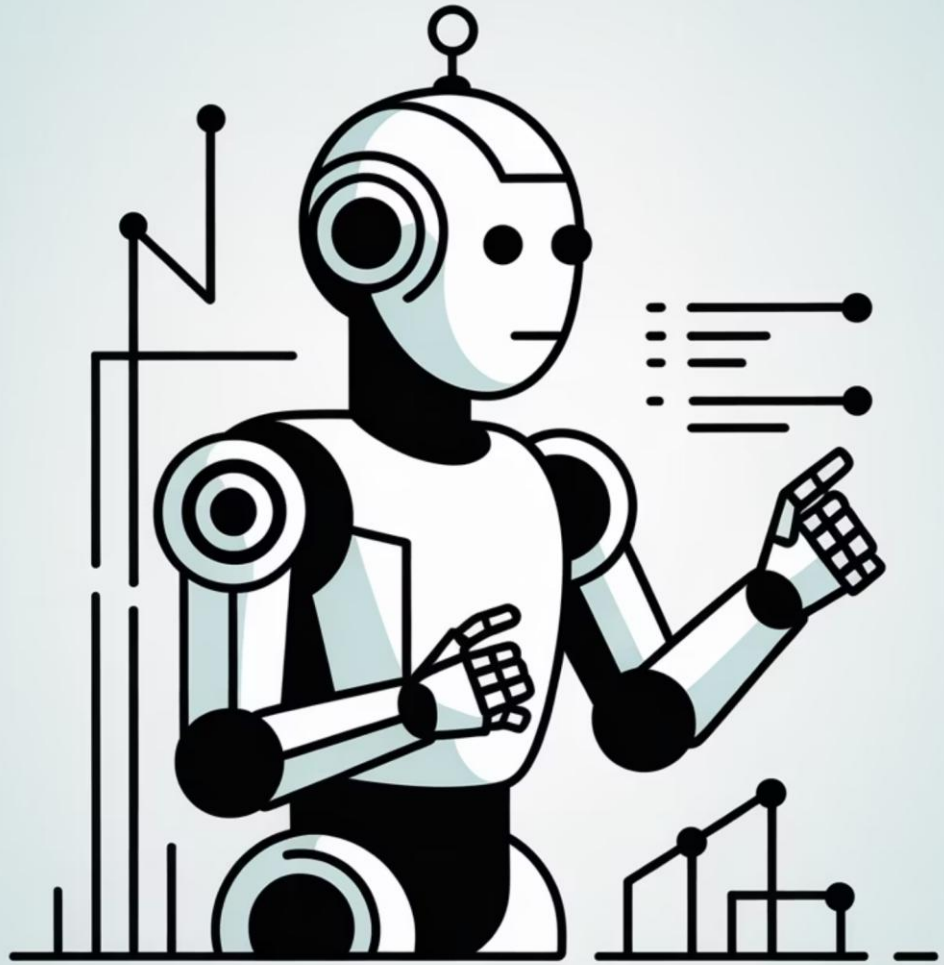
Del Gobierno del Dato al Gobierno de la Información

UDIT UNIVERSIDAD DE DISEÑO Y TECNOLOGÍA

Un Nuevo Paradigma de Ejecución

Los **Agentes de IA** están cambiando la relación entre la tecnología y el trabajo: ya no solo **analizan o recomiendan**, ahora **actúan**. Pueden buscar información, interpretar contexto, tomar decisiones, ejecutar tareas en herramientas corporativas y coordinarse con otros agentes para completar procesos end-to-end. En la práctica, esto convierte a la IA en un **nuevo tipo de "trabajador digital"** capaz de operar a escala, 24/7, y con impacto directo en operaciones, clientes y resultados.

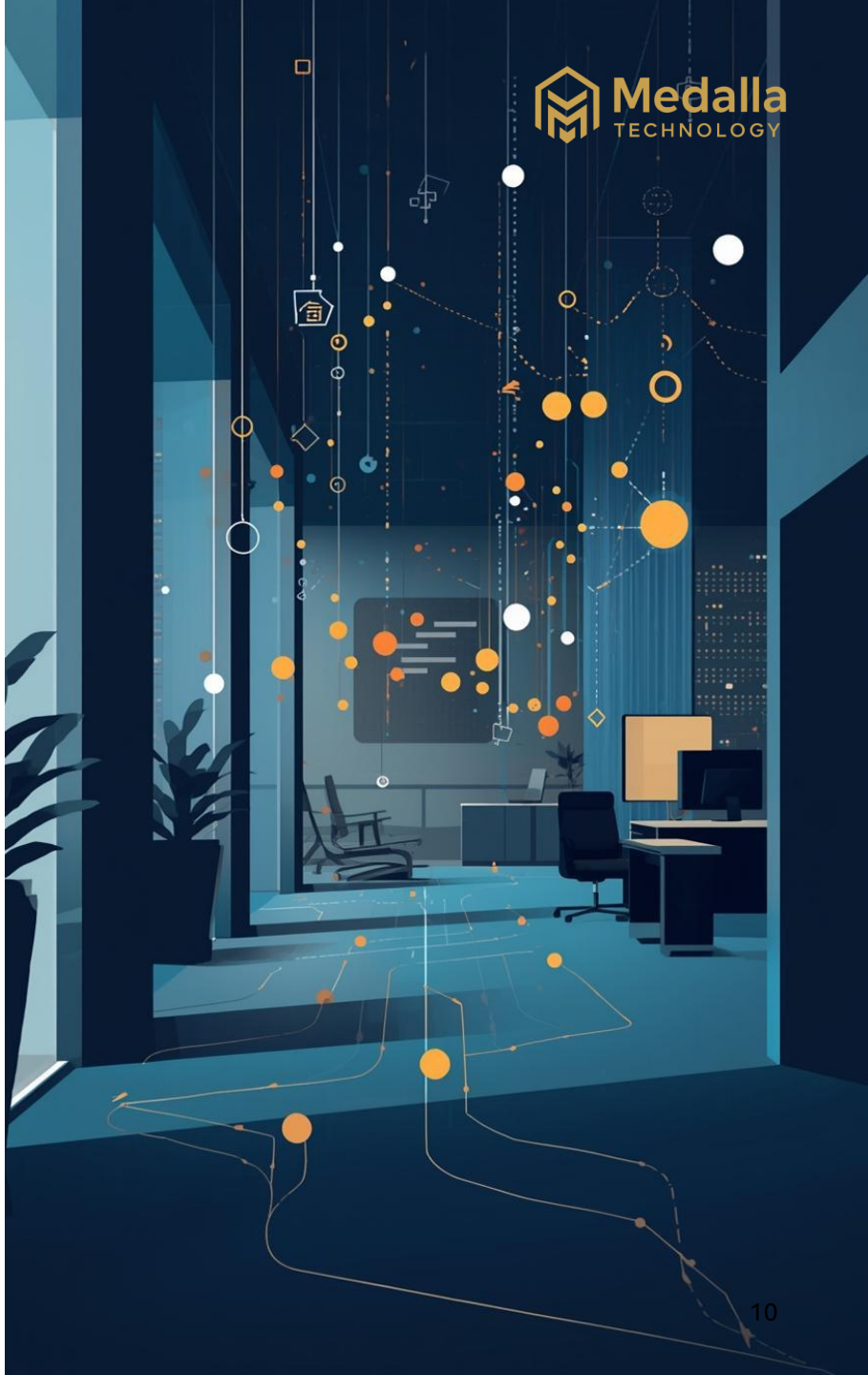
Sin embargo, este paso de "IA conversacional" a "IA autónoma" introduce **nuevos retos de gobernanza** que los **frameworks tradicionales de Gobierno del Dato o de la IA** no fueron diseñados para cubrir. Aparecen riesgos difíciles de controlar y aún más difíciles de auditar: **acciones no autorizadas**, **uso indebido de permisos**, **decisiones opacas**, **costes impredecibles** por ejecución iterativa, o agentes optimizando el objetivo equivocado sin que nadie lo detecte a tiempo.



Un Nuevo Paradigma de Información

La **Inteligencia Artificial ha revolucionado** fundamentalmente cómo las organizaciones gestionan y extraen **valor de sus activos informativos**. Ya no es necesario estructurar toda la información en bases de datos relacionales: documentos, imágenes, audio y vídeo pueden ser consumidos directamente por modelos de IA avanzados.

Sin embargo, esta democratización del acceso informacional ha creado **nuevos desafíos de gobernanza que los frameworks tradicionales de Gobierno del Dato no fueron diseñados para abordar**. Las organizaciones se enfrentan a volúmenes masivos de información no estructurada sin controles adecuados de calidad, seguridad o trazabilidad.



Nuestra visión del Ecosistema de Gobierno de la Información

En **Medalla Tech** tenemos claro que **para aprovechar al máximo los datos y tener una ventaja competitiva** de la información, no basta con implementar un modelo de gobierno del dato “tradicional”, ni si quiera con un gobierno de la IA, **es necesario tener una visión end to end** desde que se ingesta el dato hasta que se productiviza, es por ello por lo que proponemos una **visión completa Bottom-Up, que interacciona entre los distintos marcos de trabajo** propios que hemos definido.

Framework Gobierno del Dato

Framework Gobierno de la Información No Estructurada

Framework Gobierno de la Inteligencia Artificial

Framework Gobierno de los Agentes de IA

Gestión del Cambio y Capacitación

Framework Gobierno del Dato

En Medalla Tech contamos con **nuestro propio framework de Gobierno del Dato e IA**, para abordar los retos que han ido surgiendo a lo largo del tiempo en torno al dato.
Este marco de trabajo está basado en las buenas prácticas definidas por los principales frameworks de gestión del dato (DAMA, DCAM, etc.), junto con las experiencias obtenidas de los diferentes clientes donde hemos prestado servicio.
Esta personalización nos permite adaptar y optimizar nuestro modelo de trabajo según la organización, lo que consigue un **despliegue y una implementación más ágil** y certera.

Gestión del Cambio

Estrategia del Dato	**POLÍTICO**		**Diseño del Marco de Gobernanza.** Estrategia y políticas, roles, responsabilidades, modelos de relación, procesos de gobierno, etc.
Arquitectura Tecnológica	**CONSTRUCTOR**		**Definición de la Arquitectura Tecnológica.** Apoyar casos empresariales y regulatorios, permitiendo escalabilidad y evolución.
Arquitectura del Dato	**CATEDRÁTICO**		**Definición y Gestión de Arquitectura del Dato.** Diccionario de datos, glosario de términos de negocio, modelos, linaje, etc.
Calidad del Dato	**CIRUJANO**		**Gestión de la calidad de los datos.** Analizar, medir y mejorar los datos en base a su ciclo de vida y mejora continua.
Gestión de Datos Maestros	**BANQUERO**		**Gestión del Dato Maestro (MDM).** Definir y gestionar los datos críticos del negocio, permitiendo a la organización tener una única visión de la verdad.
Seguridad y Privacidad	**ANTIDISTURBIOS**		**Gestión de la seguridad del dato y la privacidad.** Clasificación, administración, auditoría del uso, etc.
Cumplimiento	**POLICIA**		**Cumplimiento legal.** Garantizar el cumplimiento legal, especialmente en GDPR, EU IA Act, DORA, y demás normativas aplicabes al ámbito del dato.
Inteligencia Artifical	**INVENTOR**		**Inteligencia Artificial.** Garantizar un uso ético de los datos y el cumplimiento legal, especialmente para evitar sesgos en los modelos de alto riesgo.

Framework
Gobierno de Información No Estructurada

Pilar 1

Arquitectura Tecnológica

La Arquitectura Tecnológica define la infraestructura donde se almacena, procesa y sirve la información no estructurada para uso de la IA, siendo flexible para gestionar formatos diversos, volúmenes masivos y procesos intensivos como embeddings y vectorización.

Pilar 2

Arquitectura de la Información

La Arquitectura de la Información organiza y hace descubrible la información no estructurada mediante principios semánticos, metadatos enriquecidos y buenos mecanismos de búsqueda, permitiendo que personas y modelos de IA encuentren lo relevante en cada momento

Pilar 3

Calidad y Confiabilidad

La Calidad y Confiabilidad en información no estructurada amplía la calidad de datos clásica incorporando veracidad temporal, contexto y posibles derivas de significado. Define cómo evaluar y asegurar que la información siga siendo correcta, relevante y fiable con el tiempo, evitando que los sistemas de IA propaguen contenido obsoleto o erróneo.

Pilar 4

Adaptabilidad

La Adaptabilidad asume que tanto la información no estructurada como los modelos de IA cambian de forma continua y exige mecanismos de ajuste permanente que el gobierno tradicional no contemplaba. Define procesos para gestionar ese cambio constante.

Pilar 5

Seguridad, Privacidad y Ética

La Seguridad, Privacidad y Ética adapta los controles clásicos al mundo no estructurado, gestionando PII incrustada en textos, derecho al olvido en embeddings y trazabilidad de qué documentos influyen en cada decisión de IA.

Pilar 6

Economía de la Información

La Economía de la Información define cómo medir el valor real de la información no estructurada y optimizar su TCO para IA, permitiendo decidir qué activos merece la pena gobernar y mantener y asegurando la sostenibilidad financiera del programa.

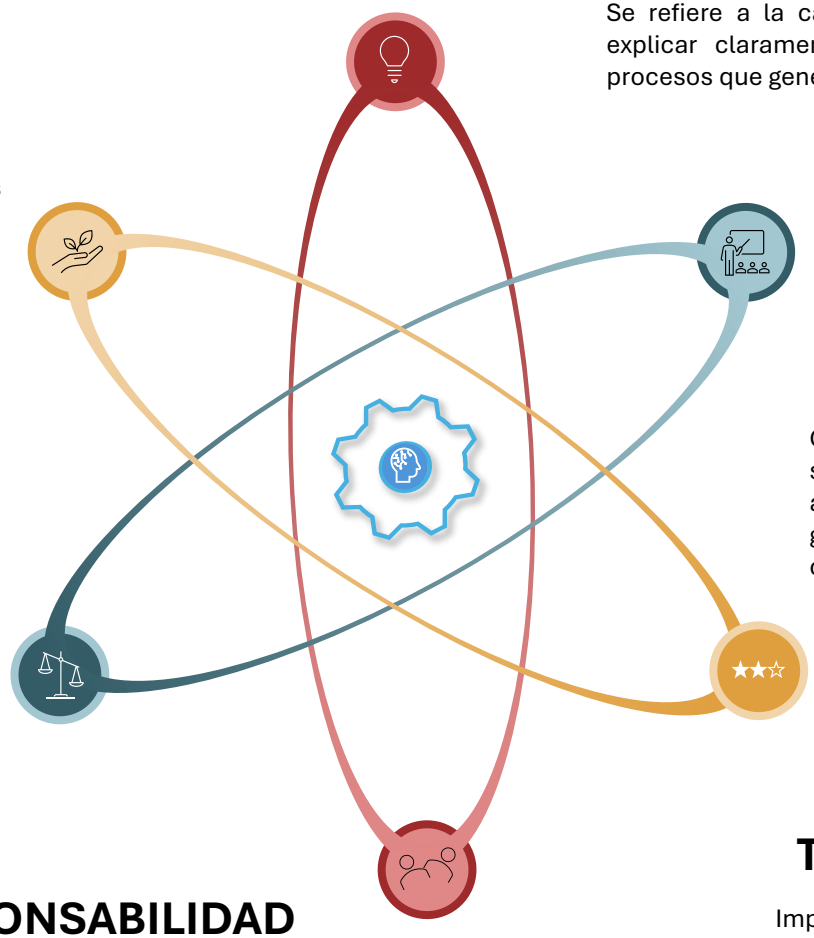
Framework Gobierno de la IA

EXPLICABILIDAD

Se refiere a la capacidad del sistema de IA para explicar claramente las decisiones, resultados y procesos que genera.

SOSTENIBILIDAD

La sostenibilidad busca que los modelos de IA sean viables a nivel energético, permitiendo medir su consumo y reducir su impacto ambiental. Se enfoca en optimizar los recursos computacionales y evaluar la huella de carbono..



TRANSPARENCIA

Garantiza que el diseño, la formación y el uso del sistema de IA sean trazables y accesibles para las auditorías. La transparencia fomenta la confianza y garantiza que los sistemas de IA puedan evaluarse objetivamente.

EQUIDAD

Se centra en garantizar que los sistemas de IA sean inclusivos y no discriminen a ningún grupo o individuo, eliminando los sesgos que puedan surgir durante el desarrollo o el uso del modelo.

TRAZABILIDAD

Implica establecer mecanismos para evaluar y verificar periódicamente el rendimiento, los resultados y el cumplimiento de la normativa de los sistemas de IA.

RESPONSABILIDAD

Implica la asignación clara de funciones y responsabilidades en el desarrollo, la aplicación y la supervisión de los sistemas de IA.

Framework Gobierno de Agentes de IA

Medalla TECHNOLOGY

Gestión del Cambio y Capacitación

Estrategia y Evaluación de Riesgos Agénticos

Define qué casos de uso son aptos para agentes, con qué nivel de autonomía y con qué tolerancia al riesgo. Incluye la clasificación de agentes y la evaluación de riesgos.

Diseño y Límites del Agente

Gobierna las decisiones de diseño que acotan el riesgo antes de que el agente opere: action-space, autonomía, contención del impacto y diseño multi-agente.

Control de Accesos y Trazabilidad Operativa

Garantiza que el agente opera con las credenciales correctas, que sus permisos están controlados, y que todo lo que hace queda registrado de forma auditable.

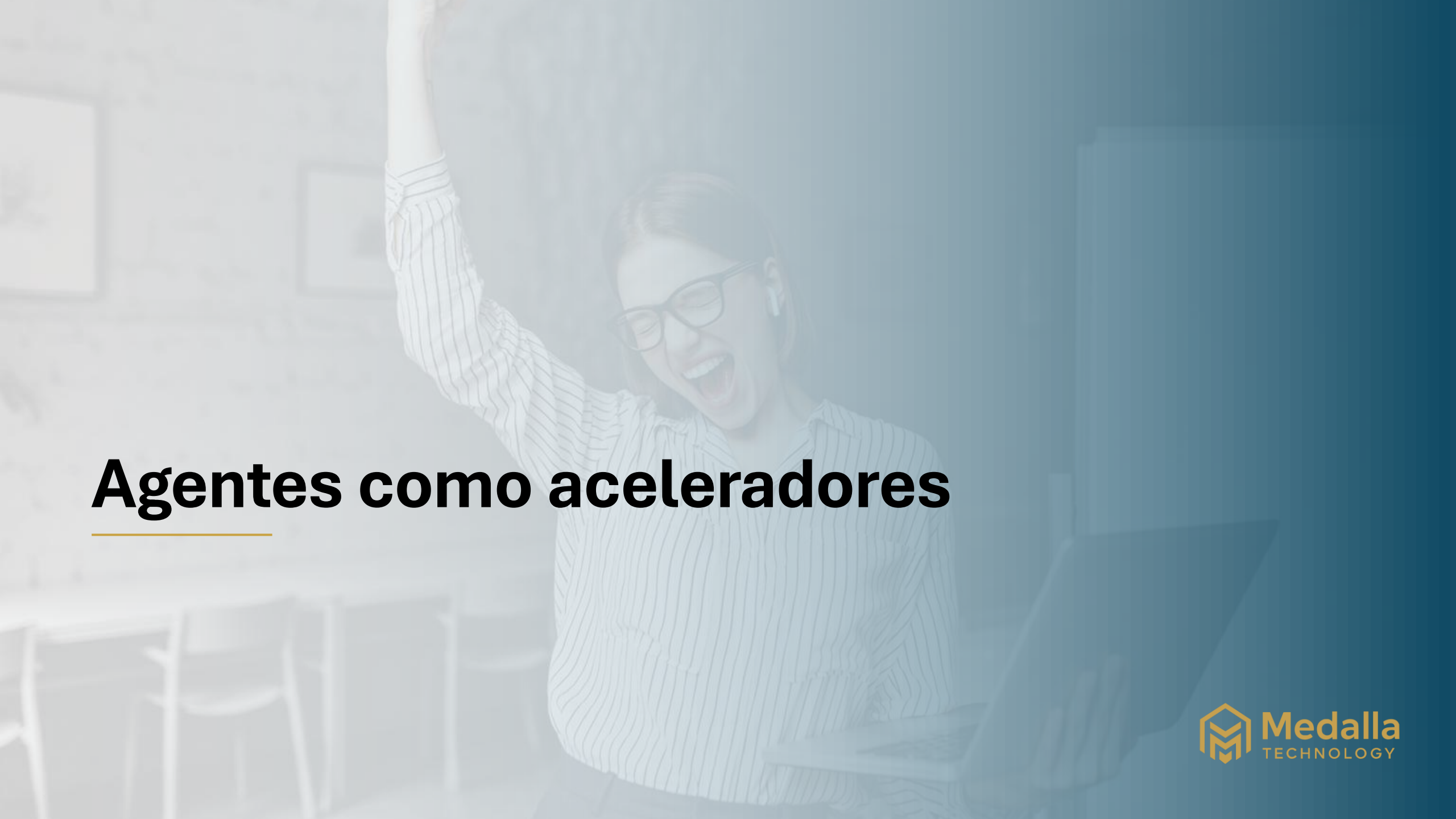
Responsabilidad y Supervisión Humana

Define quién es responsable de lo que hace el agente, cómo se ejerce la supervisión de forma efectiva y cómo se evita que esa supervisión se degrade con el tiempo.

Observabilidad

Define cómo se detecta en tiempo real que el agente se comporta según lo esperado y cómo se interviene cuando no es así.

Privacidad y Cumplimiento Normativo

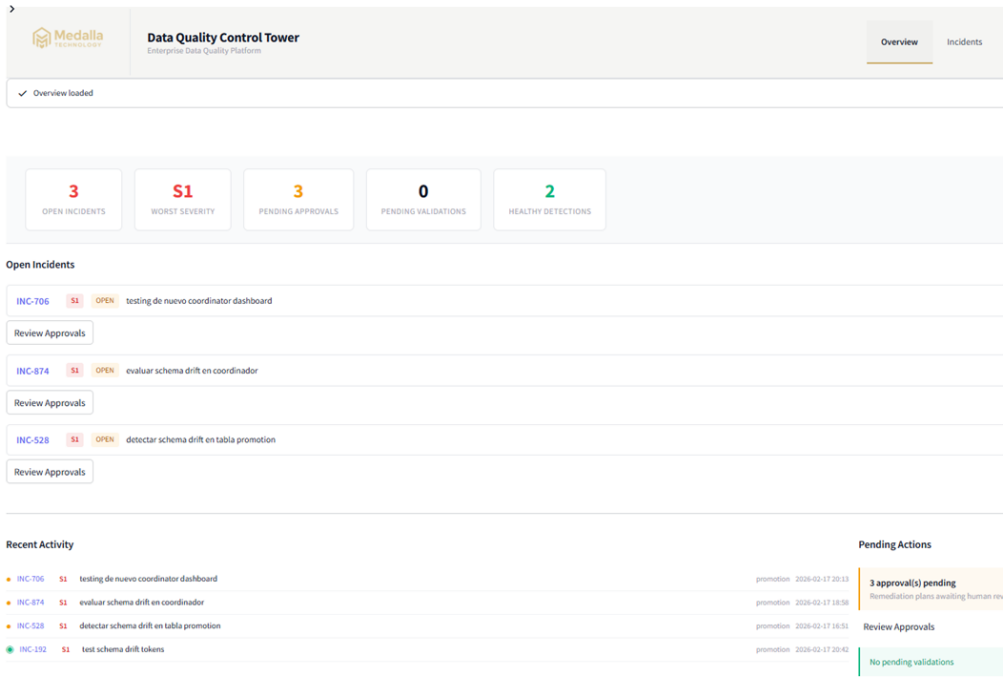


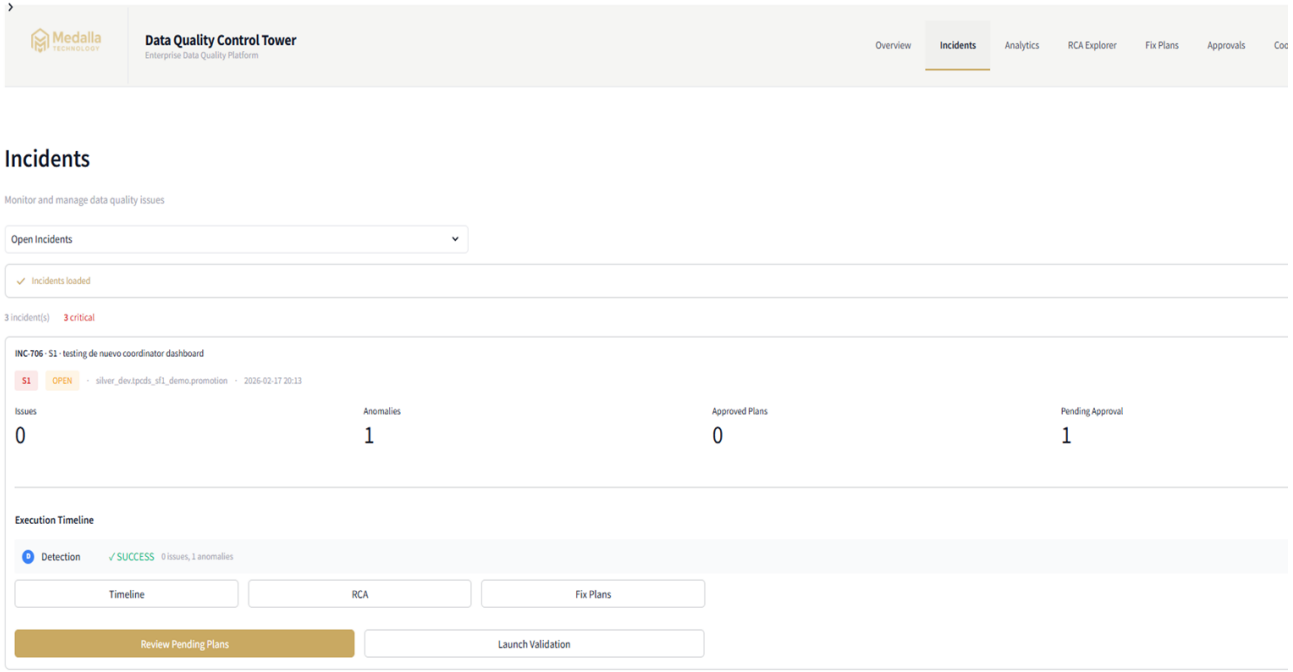
Agentes como aceleradores

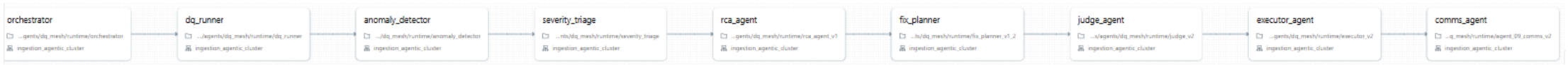
Medalla TECHNOLOGY

DQ Mesh: Sistema agéntico de calidad del dato

El sistema agéntico de calidad del dato introduce **agentes de IA especializados que monitorizan, analizan y actúan sobre la calidad de los datos de forma continua**. Estos agentes son capaces de **detectar anomalías, identificar causas raíz y proponer o ejecutar acciones de corrección, reduciendo la dependencia de procesos manuales**. De este modo, la organización evoluciona desde un enfoque reactivo hacia un modelo proactivo y autónomo de gestión de la calidad del dato, donde los problemas se anticipan y se resuelven con mayor rapidez y trazabilidad.



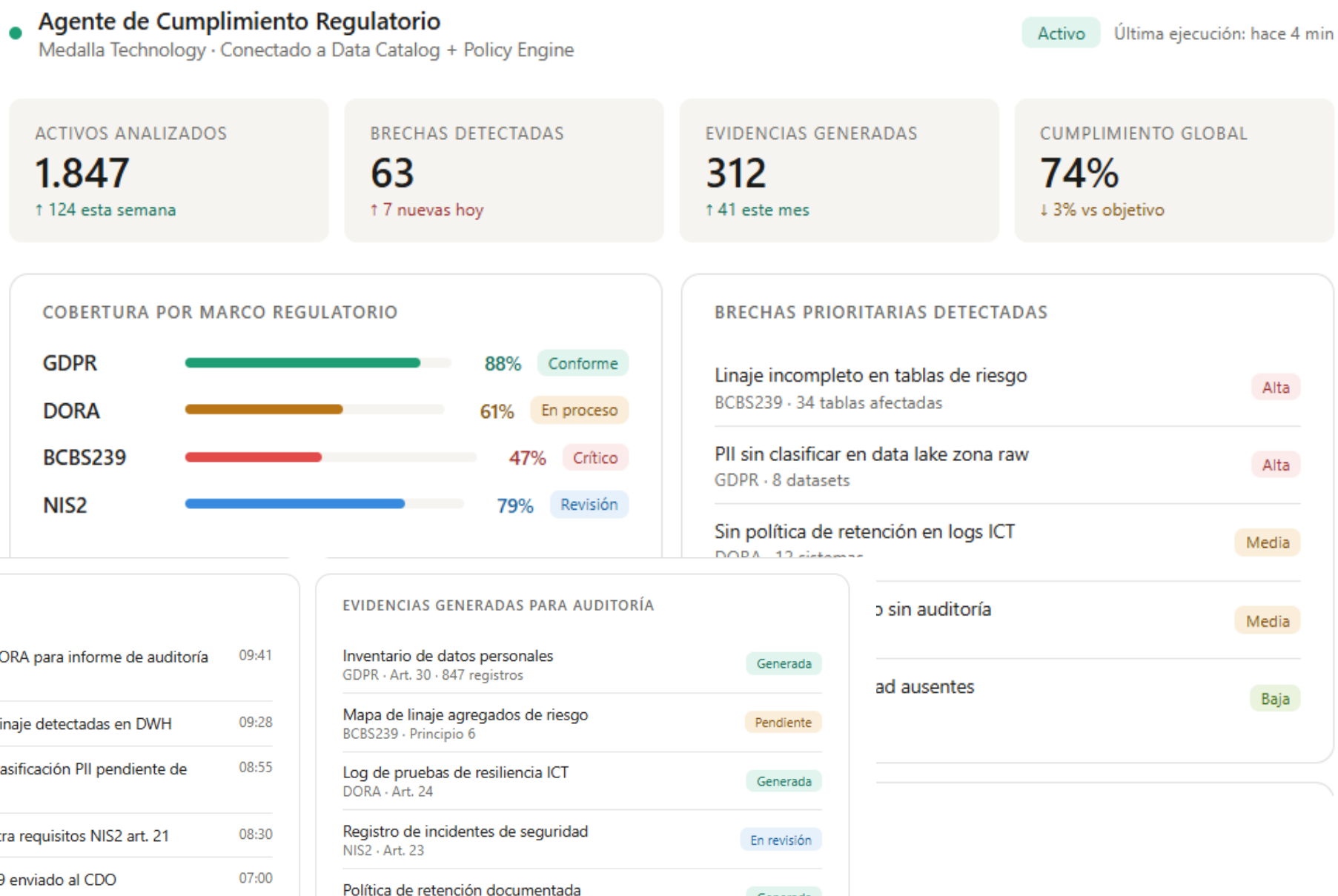




Data Product Agent

El Data Product Agent **permite a los usuarios de negocio formular en lenguaje natural necesidades de información o nuevos data products**. El agente analiza automáticamente el catálogo de datos y las tablas existentes para determinar **si la información ya está disponible o cómo podría construirse**. En caso necesario, identifica los datasets implicados, propone el **diseño lógico para generarlo y automatiza la creación de un ticket** para los equipos de IT o data engineering, facilitando así la implementación. Con ello **se reduce drásticamente el tiempo entre la necesidad de negocio y la disponibilidad del dato.**

Agente Cumplimiento Normativo



databricks

Medalla TECHNOLOGY

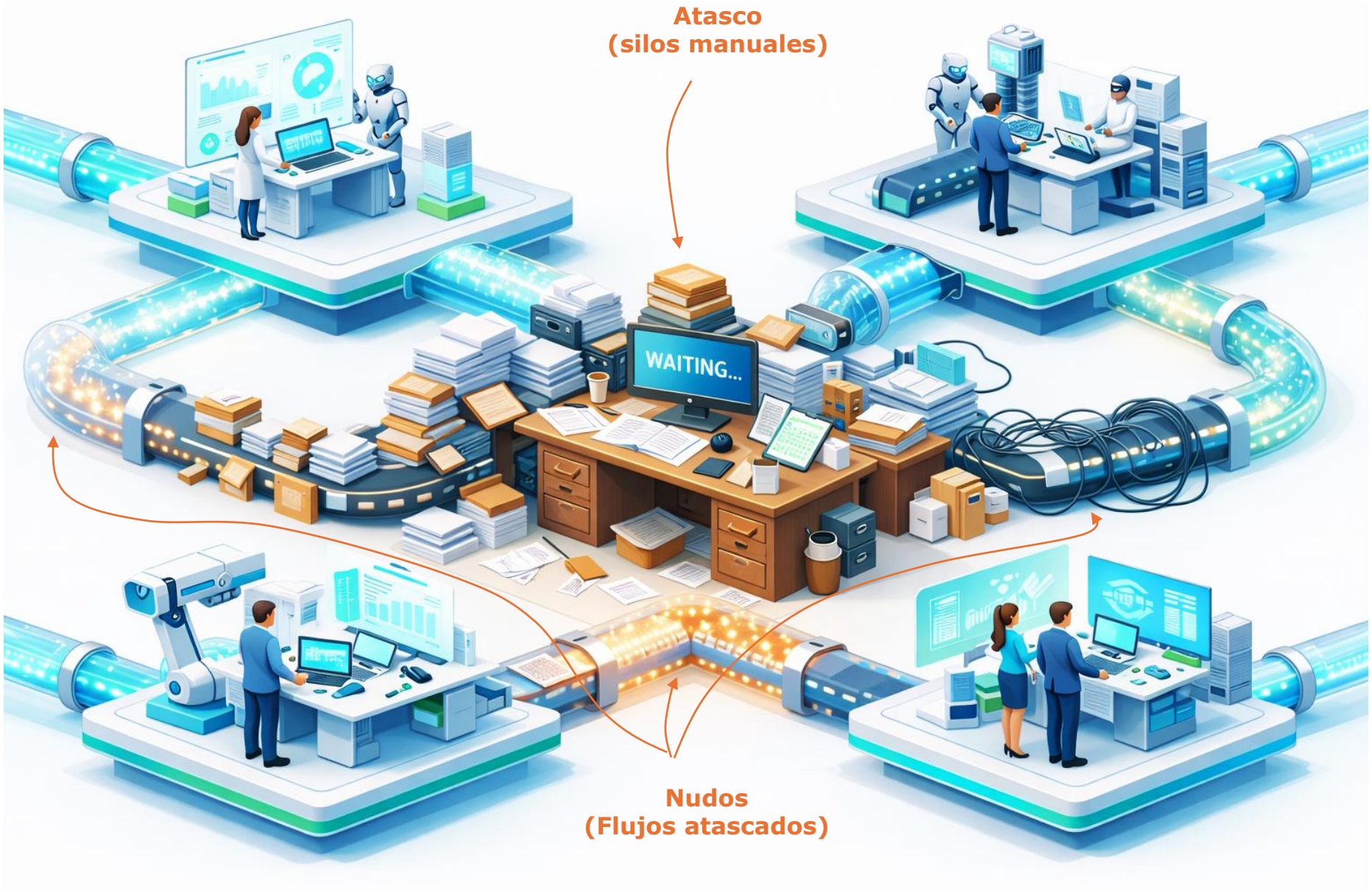
Roadmap hacia la Adopción

Primeros pasos

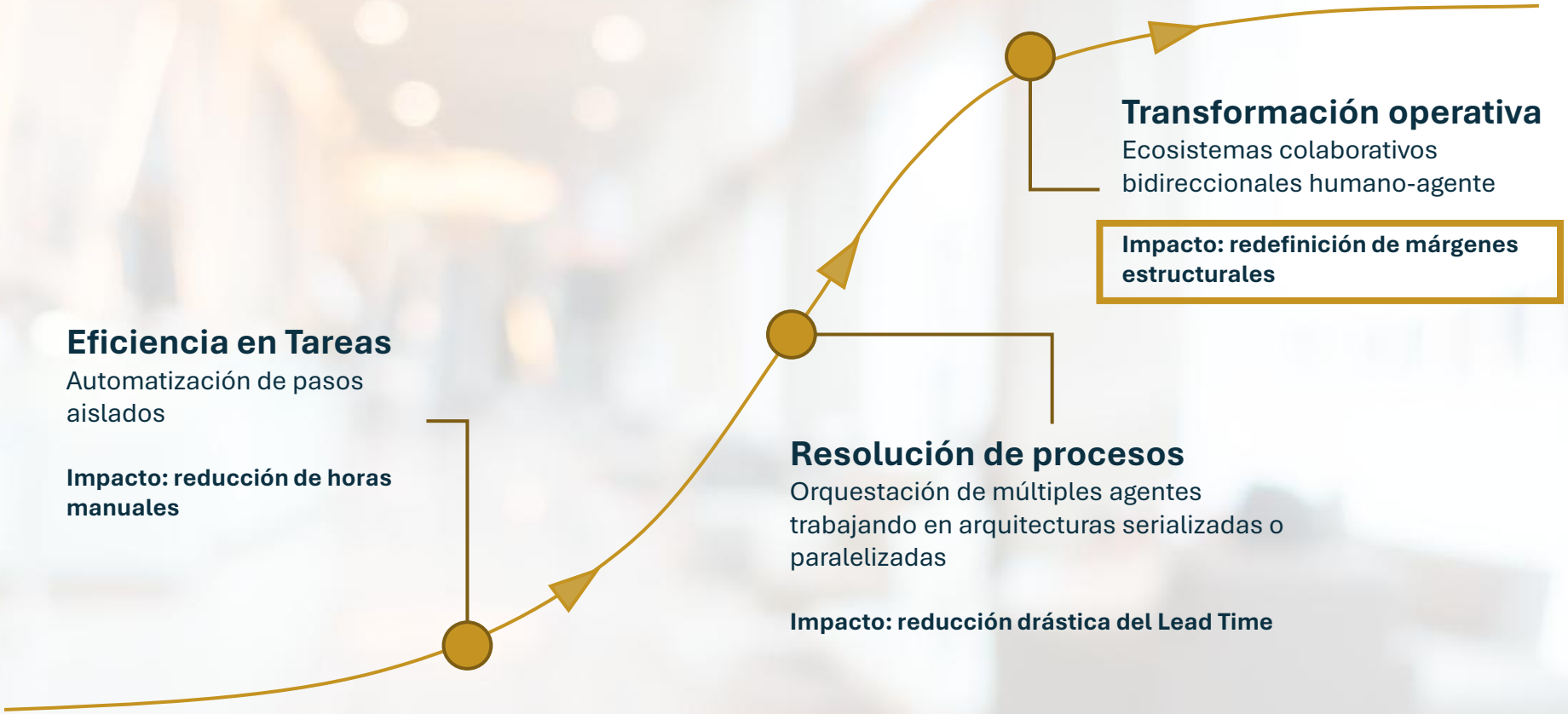
UDIT UNIVERSIDAD DE DISEÑO Y TECNOLOGÍA

1. El diseño de la automatización con IA

1. La Red de los Canales Obstruidos: nuestra organización no es perfecta

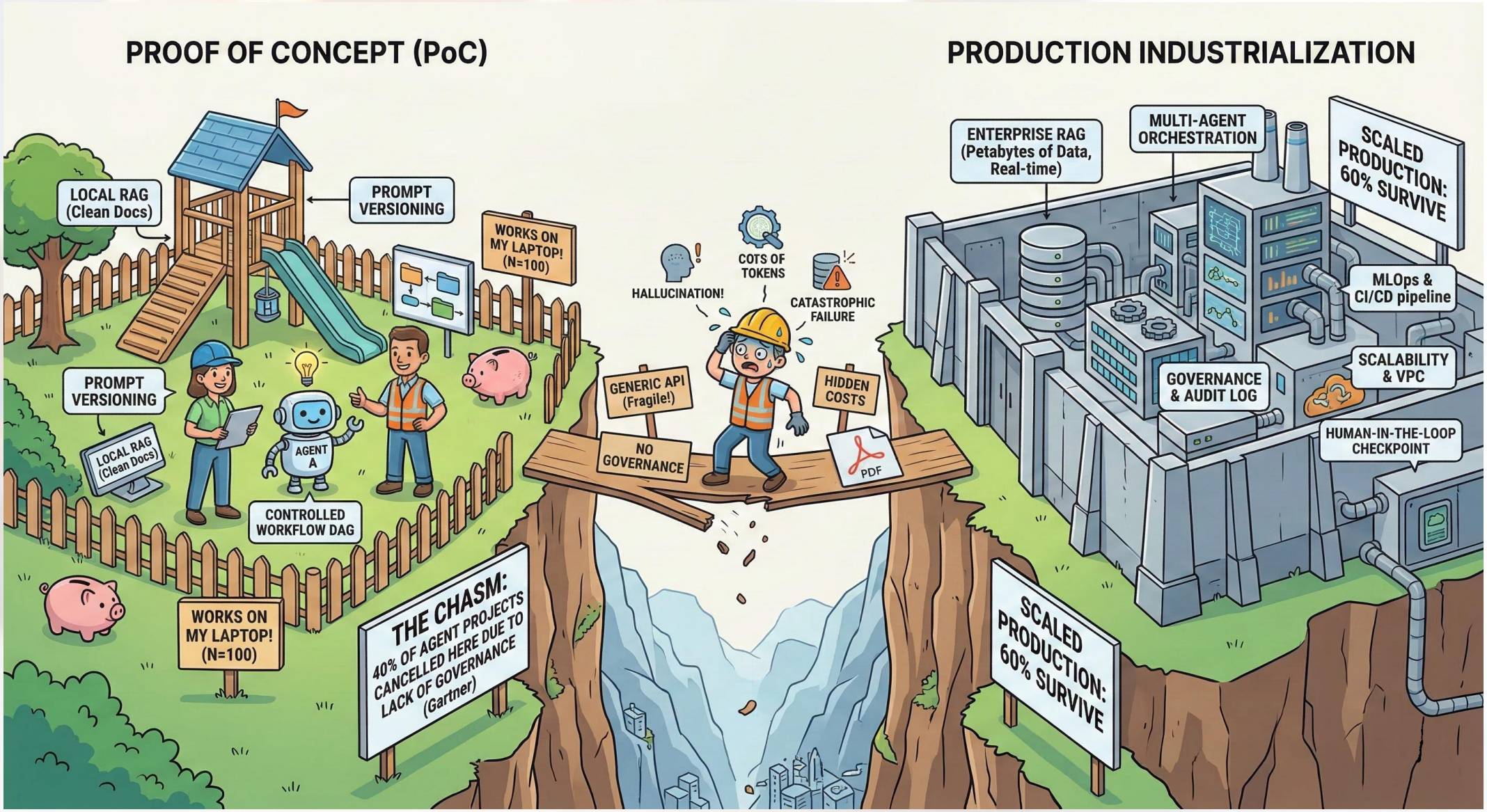


1. Generación de Valor: de la Tarea al Ecosistema



El valor real no consiste en automatizar un click, sino en orquestar un flujo de trabajo completo
En la medida que avanzamos por la curva, la gestión del cambio va tomando mayor relevancia

1. El abismo entre la Promesa y la Producción



1. Escalando Autonomía: Riesgos clave en agentes IA

Resultados impredecibles

Pérdida de confianza por **alucinaciones en procesos críticos o en entornos regulados**

Impacto sistémico

Agentes con permisos de escritura expuestos a inyecciones de prompts pueden generar **acciones destructivas** sobre ERPs o CRMs

Agentic Sprawl

Proliferación caótica de agentes desconectados (**Shadow AI**), lógica duplicada y baja visibilidad

Costes descontrolados

Consumo incontrolado de tokens o bucles infinitos de llamadas a herramientas pueden **disparar el TCO** drásticamente

En un entorno de autonomía sin control, los agentes de IA pueden escalar errores más rápido que el valor que generan

1. Matriz de Decisión: Identificación y Clasificación de Procesos

No todos los procesos deben automatizarse igual

Inferencia Determinista

Compliance estricto.
Reglas inflexibles sin alucinaciones

Solución: KG + DAG con reglas de negocio y entidades corporativas, validación post-generación

IA Agéntica Supervisada (HITL)

Decisiones financieras, despliegue de código, modificaciones directas de ERP

Solución: orquestación multiagente + HITL + AgentOps + log inmutable

Automatización Tradicional

Tareas repetitivas y estáticas sin variabilidad

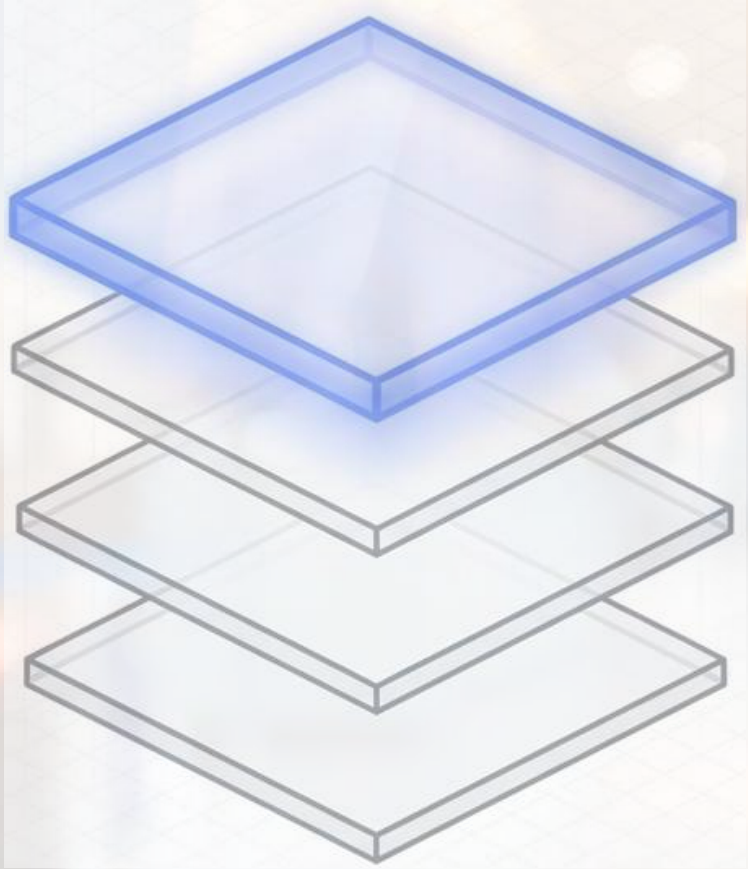
Solución: scripting determinista con orquestación simple, reglas fijas, sin IA

Agentes Autónomos

Redacción, resúmenes, clasificación de tickets soporte

Solución: RAG + agentes stateless, flujos one-shot pero con dato curado

1. Framework de Industrialización de Medalla Tech



Trust & AgentOps

- FinOps integrado
- Observabilidad en tiempo real
- Bucles de revisión humana

Gobernanza y Seguridad

- Identidades aisladas
- Control de acceso Zero Trust
- Prevención de inyección de prompts

Orquestación de Agentes

- Enrutamiento dinámico
- Memoria persistente
- Colaboración multiagente

Datos & Fundamentos

- Curación de datos corporativos
- Bases de conocimiento deterministas
- Conectores legacy

La solución a los riesgos de la IA no es un mejor LLM, es un sistema orquestado a un nivel superior

Gestión de Riesgos (guardrails)

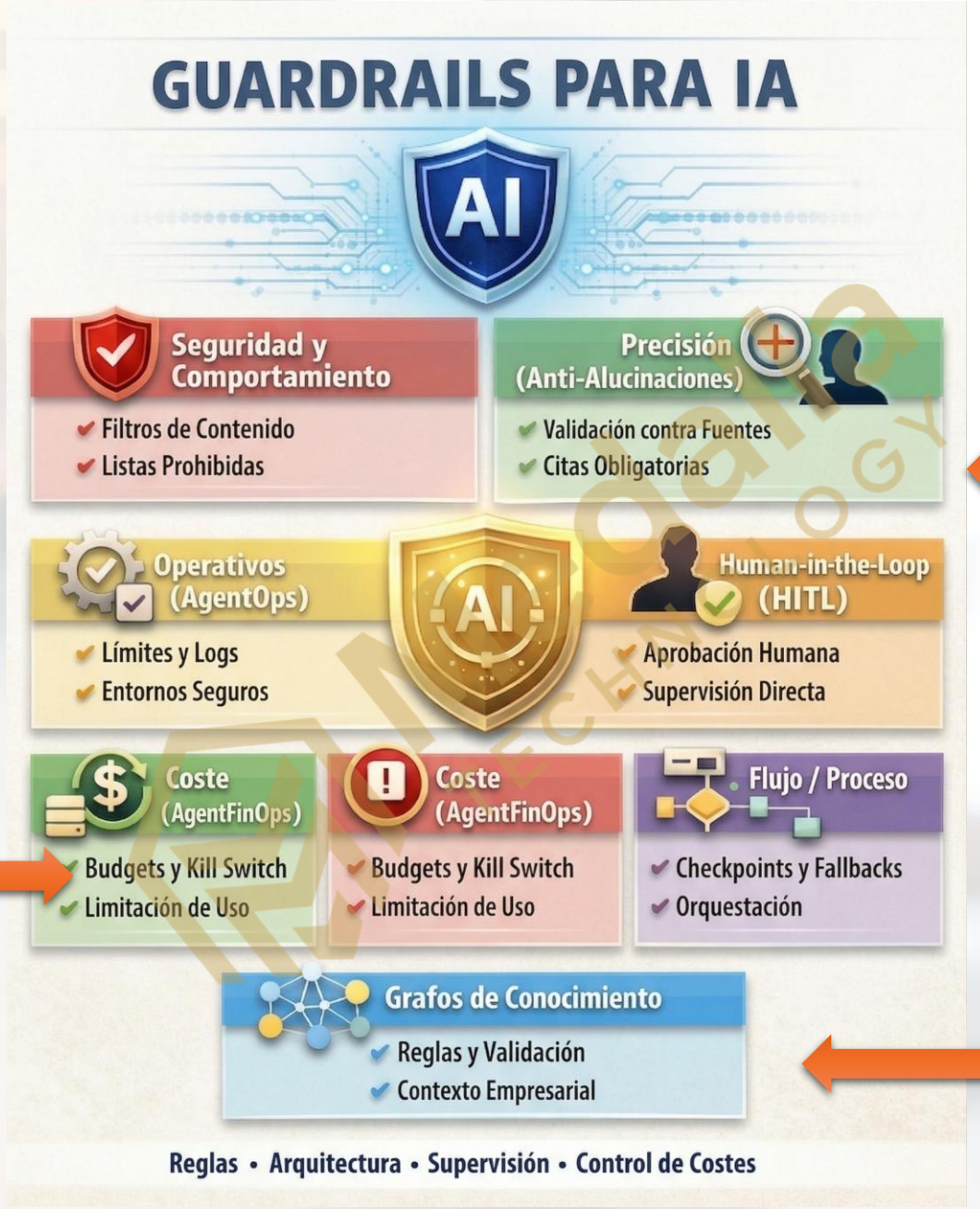
databricks

Medalla TECHNOLOGY

2. “Guardrails”

No dependen solo del modelo

Da igual lo bueno que sea nuestro modelo, en un entorno determinado y con un contexto determinado, pueda acabar fuera de control



2. HITL - El bucle “Human-in-the-Loop”

Alto impacto, alto alcance cognitivo

Medalla TECHNOLOGY

01

Proponer

El agente genera un paquete de evidencia y pausa su ejecución

02

Aprobar

El humano **revisa la evidencia en segundos**, no el proceso

03

Ejecutar

Ejecución determinista sobre las herramientas corporativas

04

Auditar

Registro inmutable guardado para compliance

Separación arquitectónica estricta: autonomía máxima en el análisis / control absoluto en la acción
Problema: hay que evaluar bien qué metermos en el bucle, perdemos una parte de la eficiencia

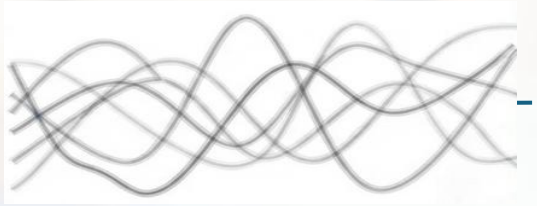
2. “Guardrails” deterministas para entornos regulatorios

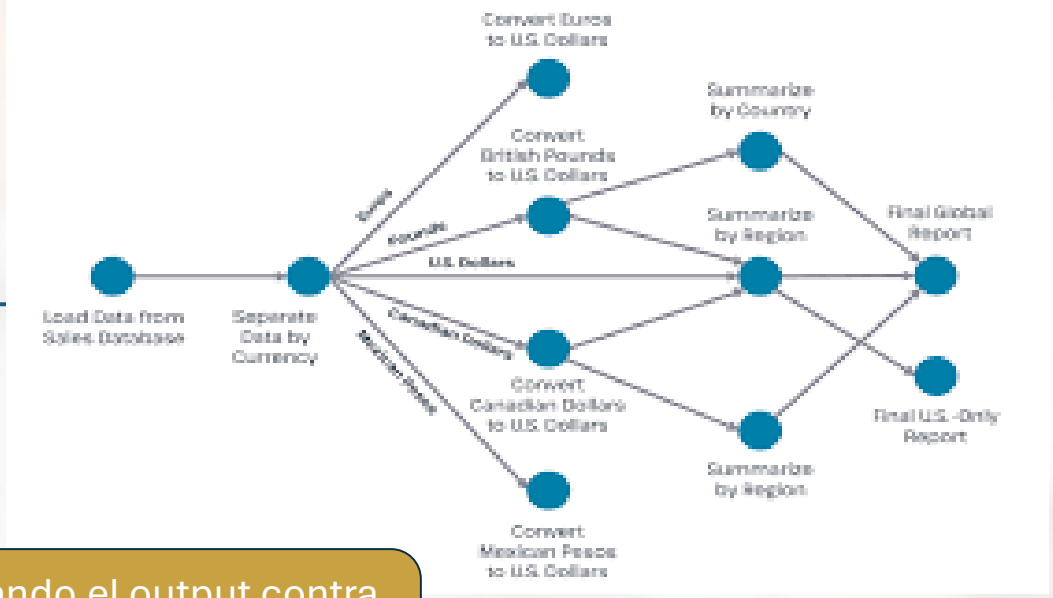
Alto impacto, poca flexibilidad

Medalla TECHNOLOGY

Grafo de Conocimiento
(Reglas y Entidades Corporativas estrictas)

Generación probabilística (LLM ruidoso)



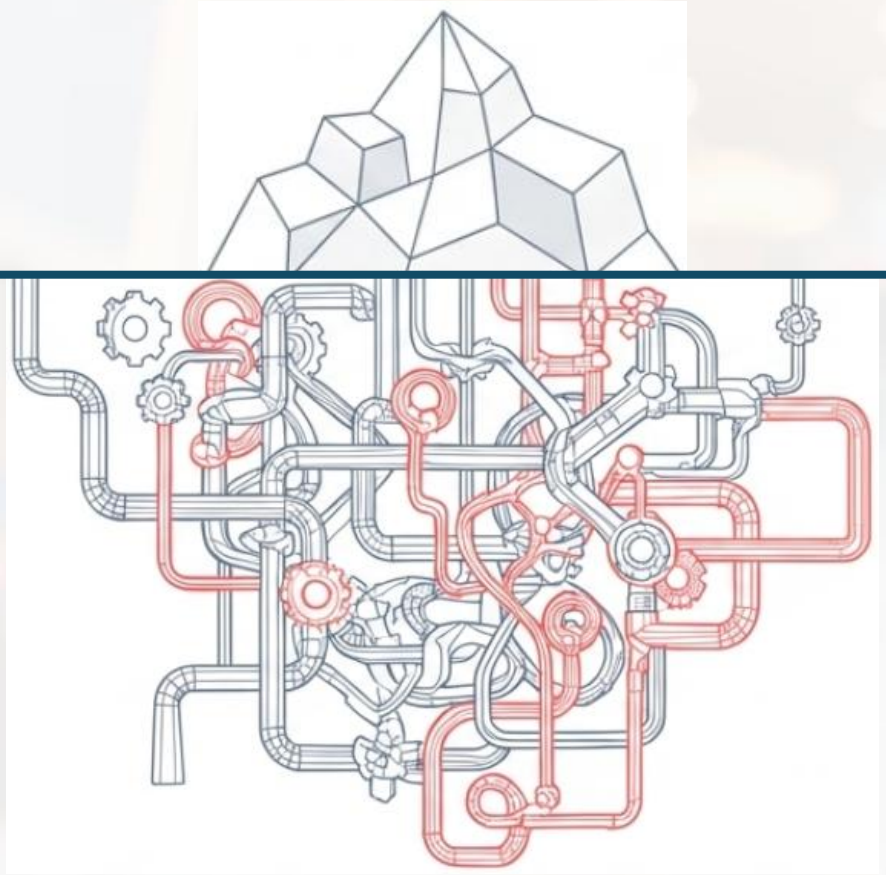


Salida Determinista y Segura

- **Validación post-generación** cruzando el output contra un Grafo de Conocimiento DAG
- Reducción drástica del número de alucinaciones
- **Posible Generación de DAG con agentes** con información desestructurada, solo supervisión humana sobre DAG

- ✓ **Restricciones semánticas**: no permitir combinaciones inválidas
- ✓ **Validación de entidades**: comprobar que los datos existen
- ✓ **Reglas de negocio explícitas**: lógica codificada fuera del modelo

2. FinOps y el verdadero TCO agéntico



Costes visibles

- Coste base por token (API LLM)
- Infraestructura y Computación estándar
- Licencias de Plataforma

Costes ocultos (el riesgo del escalamiento)

- **Bucles infinitos**: agentes atrapados en ciclos de auto-corrección fallidos.
- **Sprawl de Llamadas a Herramientas**: uso innecesario de llamadas a APIs costosas
- **Shadow IT Agéntico**: lógica duplicada en múltiples departamentos sin reutilización
- **Reintentos No Gestionados**: consumo masivo por fallos de contexto

Solución AgentFinOps: Implementación de Aceleradores, límites de gasto (throttling) por flujo de trabajo y métricas unitarias desde el principio

2. AI Agent Cost Governance (AgentFinOps)

Medalla TECHNOLOGY

CONTROL: **“Throttling” y Límites**

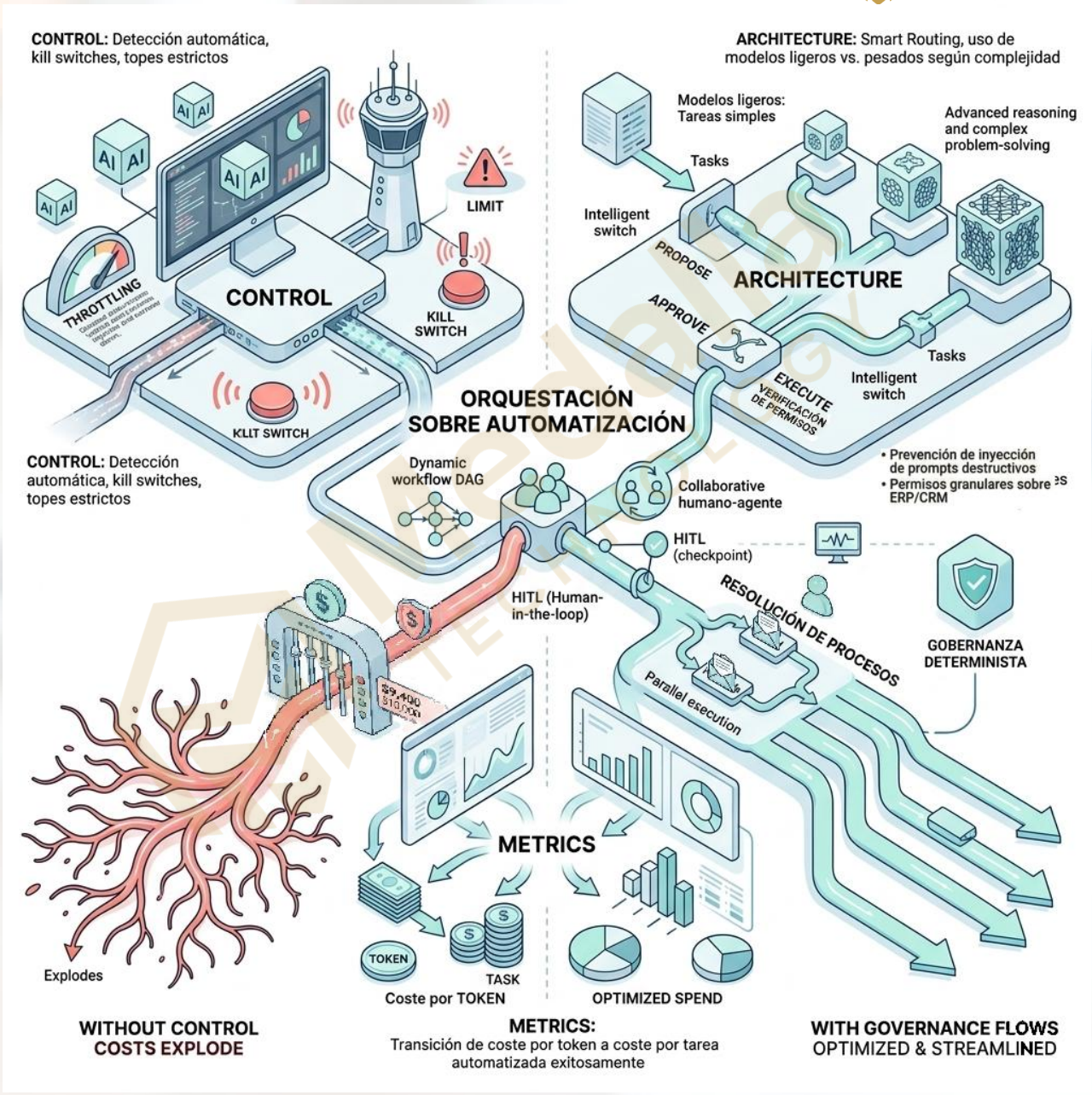
Detección automática (**kill switches de bucles infinitos** y **topes estrictos de consumo** de tokens por departamento o agente

METRICS: **Transición**

De medir el coste por “token” (que también), a medir y optimizar el “coste por Tarea automatizada exitosamente”
Gestión de alertado sobre el control

ARCHITECTURE: **Smart Routing & Quality Trade off**

Especialización de arquitecturas para diferentes flujos
Uso de modelos ligeros y baratos para tareas simples, reservando LLMs pesados solo para razonamientos complejos.
Optimización de prompts según modelo y trade off de calidad



Conclusiones

databricks

Medalla TECHNOLOGY

3. Conclusión: Orquestación de la automatización

De *tareas* a resolución de *Procesos*

01

Superar la "Eficiencia en Tareas" (automatización de pasos aislados) para lograr una verdadera "**Resolución de Procesos**" .

02

Mitigar riesgos críticos (alucinaciones, acciones destructivas, costes descontrolados) mediante "**Guardrails**" deterministas (HITL, AgentOps, DAGs)

03

La autonomía no es un cheque en blanco; visibilizar y gestionar los costes ocultos .
Evolucionar de medir el "coste por token" a optimizar el "**coste por Tarea exitosa**", implementando límites y "kill switches"

04

Seguir un enfoque estructurado y maduro para la adopción

3. Conclusiones: Nuestro método paso a paso

Medalla TECHNOLOGY

01

Audit & Assesment

Identificación de **procesos críticos,** evaluación de la **madurez de los datos y clasificación de flujos de trabajo**

02

Redesign AI-first

Rearquitectura de los flujos de trabajo

Golden rule: nunca superponer IA sobre un proceso roto

03

Building & Guardrails

Despliegue de **entornos seguros**, integrando arquitecturas de ejecución estrictas

04

Operation at scale

Monitoreo continuo (**AgentOps**), control financiero (**AgentFinOps**) y mejora en producción

Medalla
TECHNOLOGY

www.medallatech.com

contacto@medallatech.com