



Databricks Deep Dive: Enterprise-Scale AI Agents

Martes 24 de Marzo | 10:00 – 14:30





Databricks FinOps

Controlando nuestros costes

Los problemas

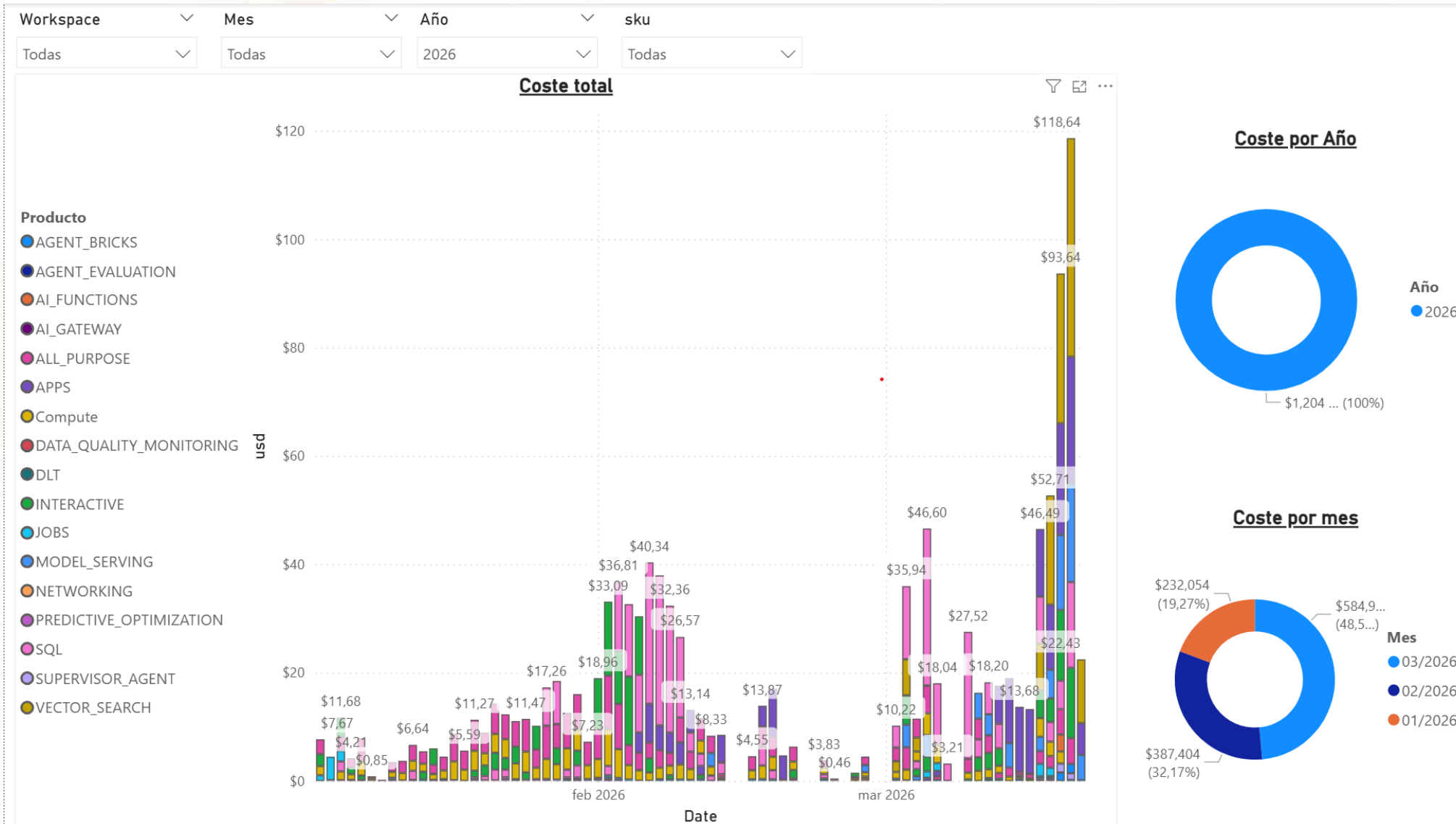
Costes no controlados.

Reparto de costes por consumidores.

Ineficiencias en la infraestructura.



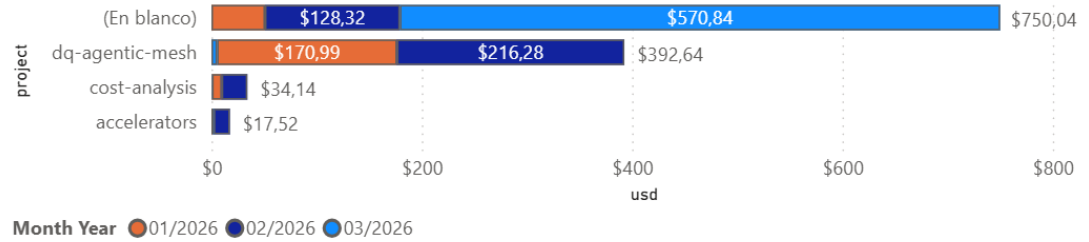
Detectamos tendencias e irregularidades de un vistazo



Organización de costes

Workspace
 Mes
 Año
 env
 project
 workload

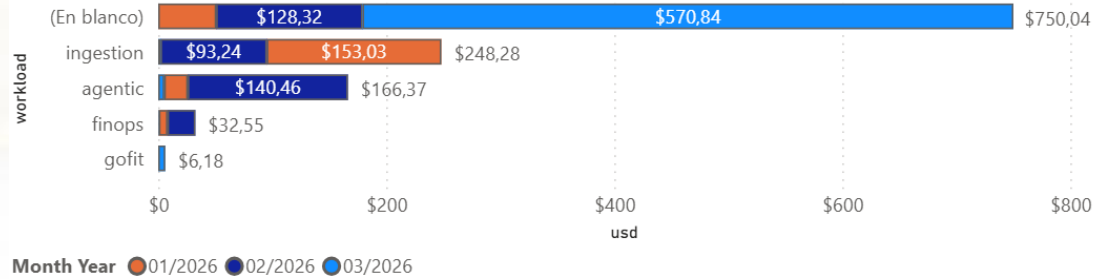
Coste por proyecto



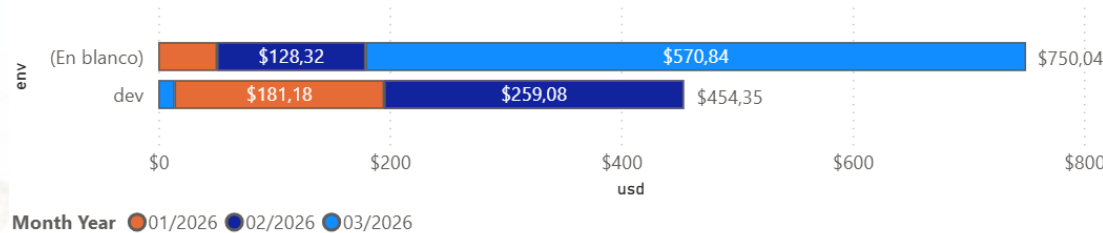
Detalles

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

Coste por workload



Coste por entorno



Total **\$1.204,388**

Análisis de ejecuciones

Job	Mes	Coste	Date	Job	Cluster	Recomendación GC	Recomendación CPU	Recomendación Memoria	Recomendación Ejecutores
Jobs Test FinOps	02/2026	\$1,258	18/02/2026	Jobs Test FinOps	0218-121721-u9qs25li	✓ Saludable	✓ CPU adecuado	● Severo: Aumentar mem...	● Subutilización moderada ...
Total		\$1,258	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

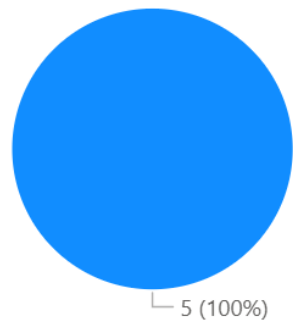
Valores recomendación memoria

- Severo: Aumentar memoria
- Crítico: Aumentar memoria
- ✓ Memoria adecuada

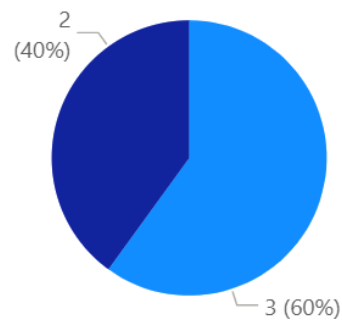
Valores recomendación workers

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

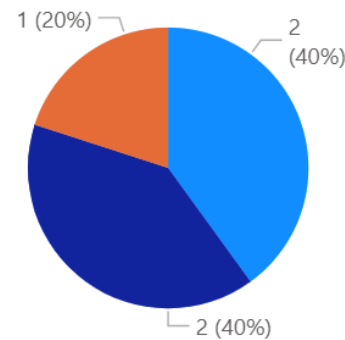
Recomendación GC



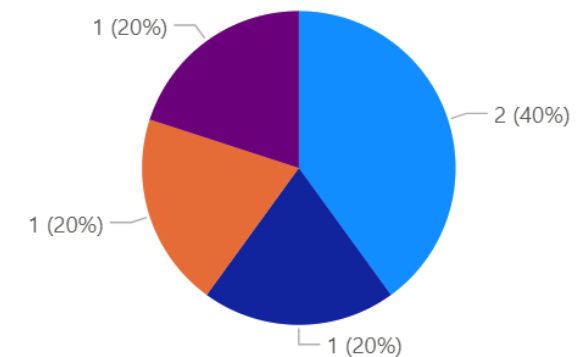
Recomendación CPU



Recomendación Memoria



Recomendación Ejecutores





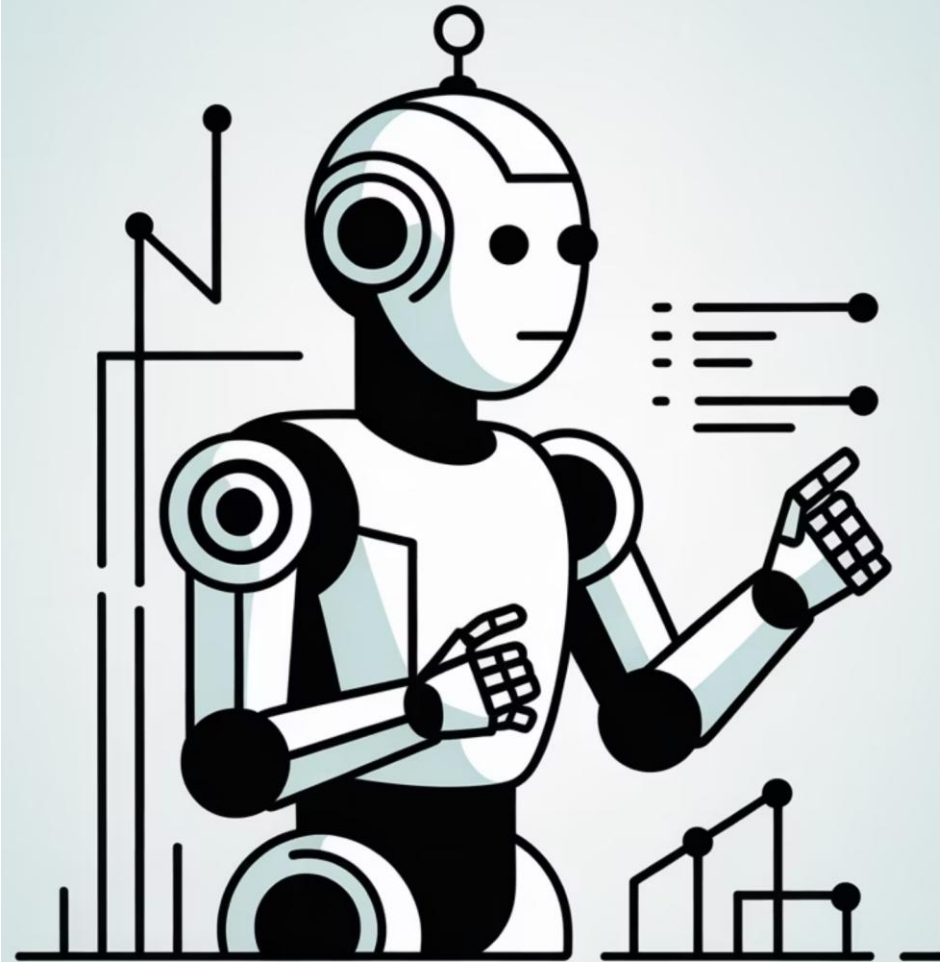
Estrategia de Datos en la era de la IA Agéntica:

Del Gobierno del Dato al Gobierno de la
Información

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 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 DDO.

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 adquiridas de los diferentes clientes durante nuestros últimos años.

Este marco de trabajo nos permite **definir, implementar, mejorar y evolucionar** los marcos de trabajo según la organización, lo que consigue un **despliegue y una implementación más ágil y sencilla**.

Estrategia del Dato	PAFIDIO	Modelo del Marco de Gobierno. Con el que se definen roles, responsabilidades, modelos de trabajo y procesos de gobierno de datos.
Implementación y Operación	CONSTRUCTOR	Definición de la Arquitectura Tecnológica. A partir de casos empresariales y tecnológicos, se definen los requisitos tecnológicos.
Adquisición del Dato	CATEGORICO	Definición y Gestión de Fuentes de Datos. Documento de datos, gestión de contratos y gestión de proveedores.
Calidad de Datos	CRUJIANO	Modelo de Calidad de los Datos. Análisis, mediciones y reportes de datos en tiempo real.
Gestión de Datos Maestros	BAJERUDO	Modelo de Datos Maestros (MDM). Define y gestiona los datos de referencia de negocio, permitiendo una integración con una plataforma de negocio.
Seguridad y Privacidad	ANTIDESTRIBIDO	Modelo de Seguridad del Dato y la Privacidad. Clasificación, administración, auditoría del uso, etc.
Clasificación	PIQUISA	Compliance Legal. Garantiza el cumplimiento legal, respaldado en GDPR, RGPD, LOPD, etc., en todos los procesos de adquisición, almacenamiento y procesamiento de datos.
Inteligencia Artificial	INVENTOR	Inteligencia Artificial. Consiste en un flujo de trabajo de cumplimiento legal, respaldado en una plataforma de negocio de alto riesgo.

Framework Gobierno de la Información No Estructurada

Framework Gobierno de Información No Estructurada

Arquitectura Tecnológica	Arquitectura de la Información	Calidad y Confiabilidad	Adaptabilidad	Seguridad, Privacidad y Ética	Economía de la Información
---------------------------------	---------------------------------------	--------------------------------	----------------------	--------------------------------------	-----------------------------------

Framework Gobierno de la Inteligencia Artificial

4. Framework Gobierno de la IA

SOSTENIBILIDAD
La sostenibilidad surge que los modelos de IA sean viables a nivel económico, ambiental y social, asegurando los riesgos que pueden surgir durante el desarrollo de estos modelos.

EXPLICABILIDAD
Se refiere a la capacidad del sistema de IA que explica, interpreta los procesos, modelos y resultados generados.

TRANSPARENCIA
Se refiere a que el modelo de IA sea transparente y accesible para los usuarios. La transparencia incluye la claridad y gestión que los usuarios de IA pueden visualizar y comprender.

EQUIDAD
Se refiere a garantizar que los modelos de IA sean justos y no discriminatorios, evitando los sesgos que pueden surgir durante el desarrollo de estos modelos.

RESPONSABILIDAD
Define la asignación clara de tareas y responsabilidades en el desarrollo, implementación y operación de los modelos de IA.

Framework Gobierno de los Agentes de IA

Framework Agentes de IA

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 afectan el riesgo antes de que el agente opere: acción-espacio, autonomía, contención del impacto y diseño multi-agente.
Control de Accesos y Trazabilidad Operativa	Garantiza que el agente opere con las credenciales correctas, que sus permisos estén actualizados, y que todo lo que hace quede 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 comporte según lo esperado y cómo se interviene cuando no es así.

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 aplicables al ámbito del dato.
Inteligencia Artificial	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.

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..

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.

RESPONSABILIDAD

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

EXPLICABILIDAD

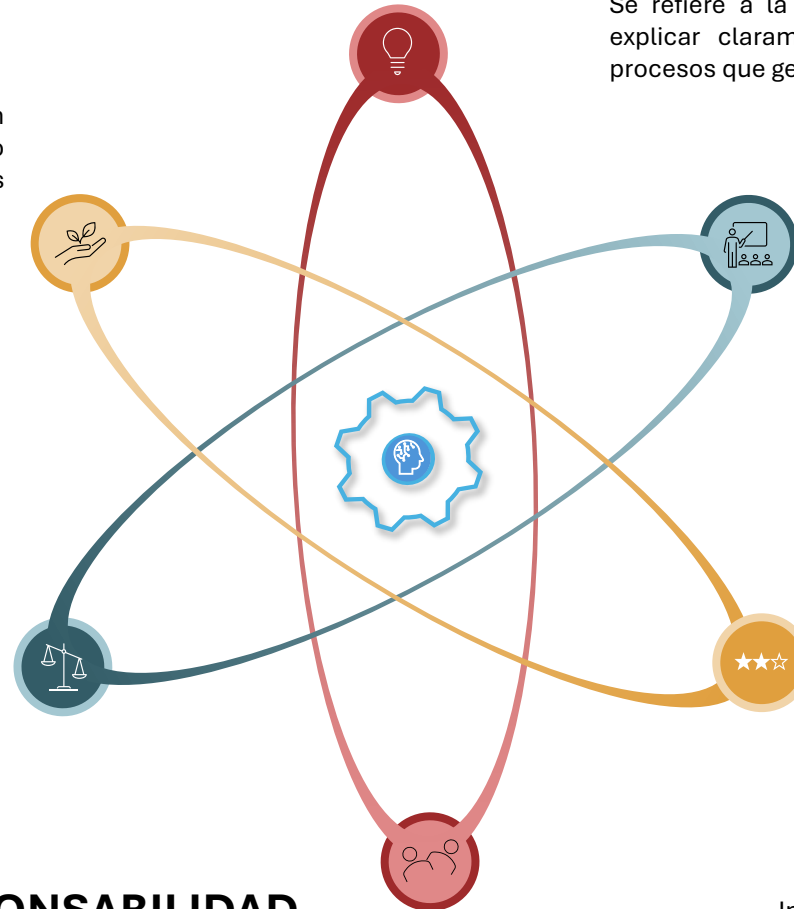
Se refiere a la capacidad del sistema de IA para explicar claramente las decisiones, resultados y procesos que genera.

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.

TRAZABILIDAD

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



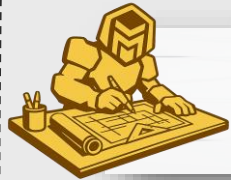
Framework Gobierno de Agentes de IA

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

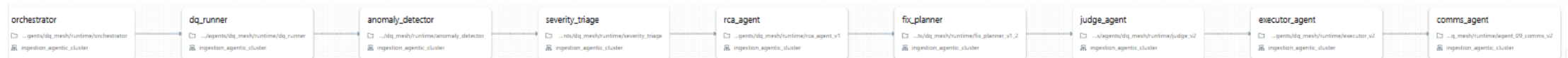
Agentes como aceleradores

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.

The screenshot shows the 'Overview' tab of the Data Quality Control Tower. At the top, there are navigation tabs for 'Overview' and 'Incidents'. Below the header, a status bar indicates 'Overview loaded'. The main content area features five summary cards: '3 OPEN INCIDENTS', 'S1 WORST SEVERITY', '3 PENDING APPROVALS', '0 PENDING VALIDATIONS', and '2 HEALTHY DETECTIONS'. Below these cards, the 'Open Incidents' section lists three items: INC-706 (testing de nuevo coordinador dashboard), INC-874 (evaluar schema drift en coordinador), and INC-528 (detectar schema drift en tabla promotion). Each item has a 'Review Approvals' button. The 'Recent Activity' section shows a log of these incidents with their respective timestamps and promotion details. On the right, the 'Pending Actions' section shows '3 approval(s) pending' and 'No pending validations'.

The screenshot shows the 'Incidents' tab of the Data Quality Control Tower. The header includes navigation tabs for 'Overview', 'Incidents', 'Analytics', 'RCA Explorer', 'Fix Plans', 'Approvals', and 'Coc'. Below the header, a status bar indicates 'Incidents loaded'. The main content area features a dropdown menu for 'Open Incidents' and a summary bar showing '3 incident(s) 3 critical'. The 'INC-706 - S1 - testing de nuevo coordinador dashboard' incident is highlighted, showing its severity (S1), status (OPEN), and associated environment (silver_dev(ipcdi_sf1_demo.promotion) - 2026-02-17 20:13). Below this, a summary bar shows 'Issues: 0', 'Anomalies: 1', 'Approved Plans: 0', and 'Pending Approval: 1'. The 'Execution Timeline' section shows a 'Detection' step with a 'SUCCESS' status, indicating '0 issues, 1 anomalies'. Below the timeline, there are buttons for 'Timeline', 'RCA', 'Fix Plans', 'Review Pending Plans', and 'Launch Validation'.



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**.

Petición del usuario

quiero una tabla que me diga quienes son los clientes que han comprado en el último año, que método de pago usaron y cuanto se gastaron

EJECUTAR AGENTE

Mensaje del Agente

No existe la tabla exacta, pero se puede crear con las tablas relacionadas.

Sugerencia de construcción

```
SELECT
  c.customer_id,
  c.first_name,
  c.last_name,
  c.email,
  p.payment_method,
  SUM(p.amount - COALESCE(p.refund_amount, 0)) AS total_spent,
  COUNT(DISTINCT o.order_id) AS orders_count
FROM test_db.customers AS c
JOIN test_db.orders AS o
  ON o.customer_id = c.customer_id
JOIN test_db.payments AS p
  ON p.order_id = o.order_id
WHERE o.order_date >= (NOW() - INTERVAL 1 YEAR)
GROUP BY
  c.customer_id,
  c.first_name,
  c.last_name,
  c.email,
  p.payment_method
ORDER BY total_spent DESC;
```

Tablas Relacionadas

compras ---> Detalle de los productos incluidos en cada pedido. Relaciona pedidos con productos específicos, cantidades y precios unitarios.
orders ---> Registro de pedidos realizados por los clientes. Contiene el estado del pedido, montos totales y dirección de envío.
payments ---> Registro de transacciones de pago asociadas a pedidos. Gestiona diferentes métodos de pago, estados de transacción y reembolsos.
products ---> Catálogo de productos disponibles para la venta. Incluye información de precios, stock, categorías y descripciones detalladas.
reviews ---> Sistema de valoraciones y reseñas de productos por parte de los clientes. Incluye calificaciones de 1-5 estrellas, comentarios y verificación de compra.
shipments ---> Sistema de seguimiento de envíos. Almacena información de transportistas, números de tracking, estados de entrega y fechas.

Resultado

customer_id	first_name	last_name	email	payment_method	total_spent	orders_count
14	Elena	Ramírez	elena.ramirez@email.com	credit_card	1679.97	1
5	Pedro	Alvarez	pedro.sanchez@email.com	credit_card	1649.98	1
2	María	García	maria.garcia@email.com	paypal	1199.99	1

CREAR TICKET

Ticket creado exitosamente
SCRUM-95
<https://medallatech.atlassian.net/browse/SCRUM-95>

Agente Cumplimiento Normativo

Agente de Cumplimiento Regulatorio

Medalla Technology · Conectado a Data Catalog + Policy Engine

Activo

Última ejecución: hace 4 min

ACTIVOS ANALIZADOS

1.847

↑ 124 esta semana

BRECHAS DETECTADAS

63

↑ 7 nuevas hoy

EVIDENCIAS GENERADAS

312

↑ 41 este mes

CUMPLIMIENTO GLOBAL

74%

↓ 3% vs objetivo

COBERTURA POR MARCO REGULATORIO

GDPR 88% Conforme

DORA 61% En proceso

BCBS239 47% Crítico

NIS2 79% Revisión

BRECHAS PRIORITARIAS DETECTADAS

Linaje incompleto en tablas de riesgo
BCBS239 · 34 tablas afectadas Alta

PII sin clasificar en data lake zona raw
GDPR · 8 datasets Alta

Sin política de retención en logs ICT
DORA · 12 sistemas Media

ACTIVIDAD DEL AGENTE

- Generadas 14 evidencias DORA para informe de auditoría Q1 09:41
- Alerta: 7 nuevas tablas sin linaje detectadas en DWH 09:28
- Escalado a Data Steward: clasificación PII pendiente de validación 08:55
- Mapeados 312 activos contra requisitos NIS2 art. 21 08:30
- Informe de brecha BCBS239 enviado al CDO 07:00

EVIDENCIAS GENERADAS PARA AUDITORÍA

- Inventario de datos personales
GDPR · Art. 30 · 847 registros Generada
- Mapa de linaje agregados de riesgo
BCBS239 · Principio 6 Pendiente
- Log de pruebas de resiliencia ICT
DORA · Art. 24 Generada
- Registro de incidentes de seguridad
NIS2 · Art. 23 En revisión
- Política de retención documentada Generada

- 3 sin auditoría Media
- ad ausentes Baja



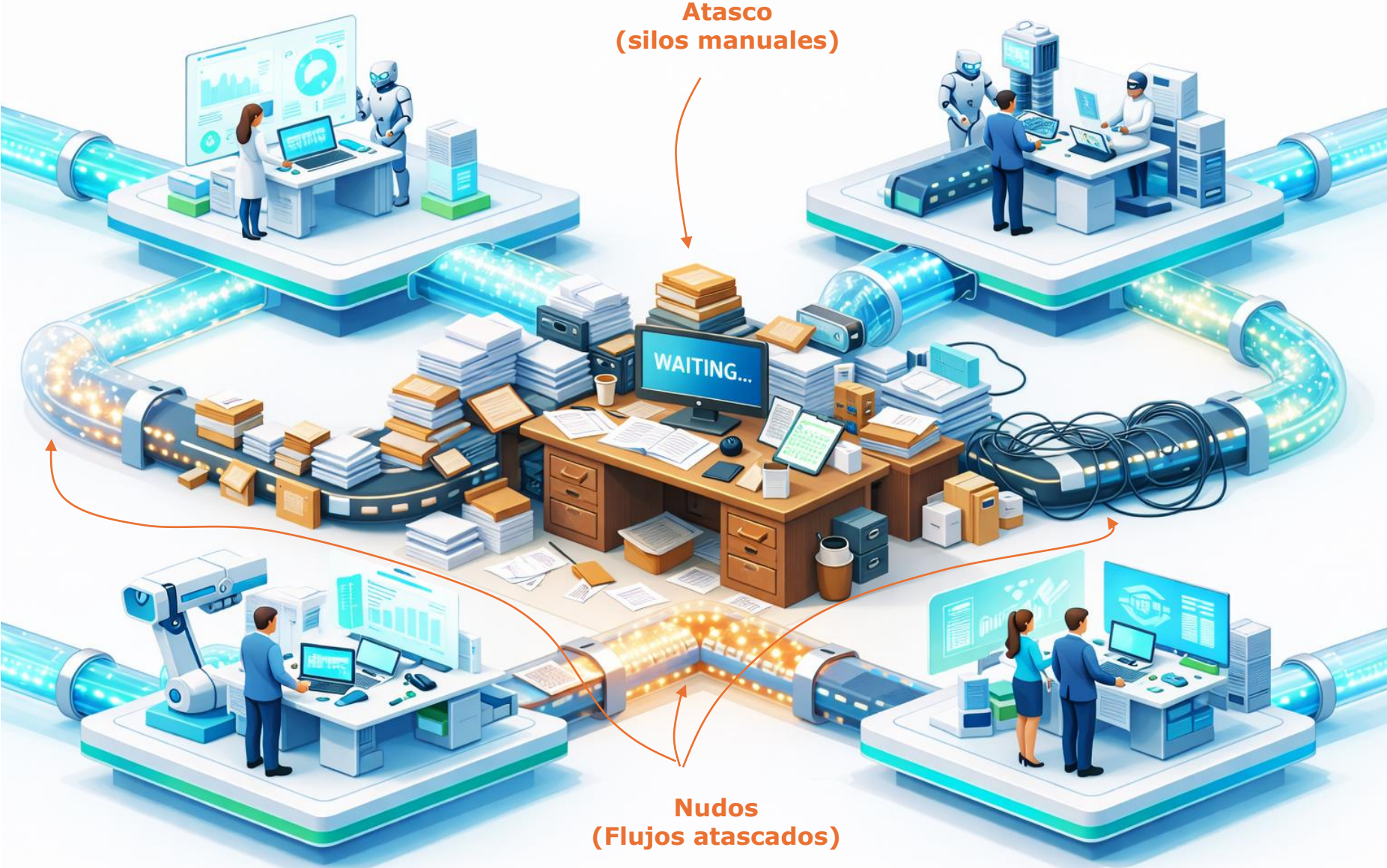
Roadmap hacia la Adopción

Primeros pasos

1. El diseño de la automatización con IA



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

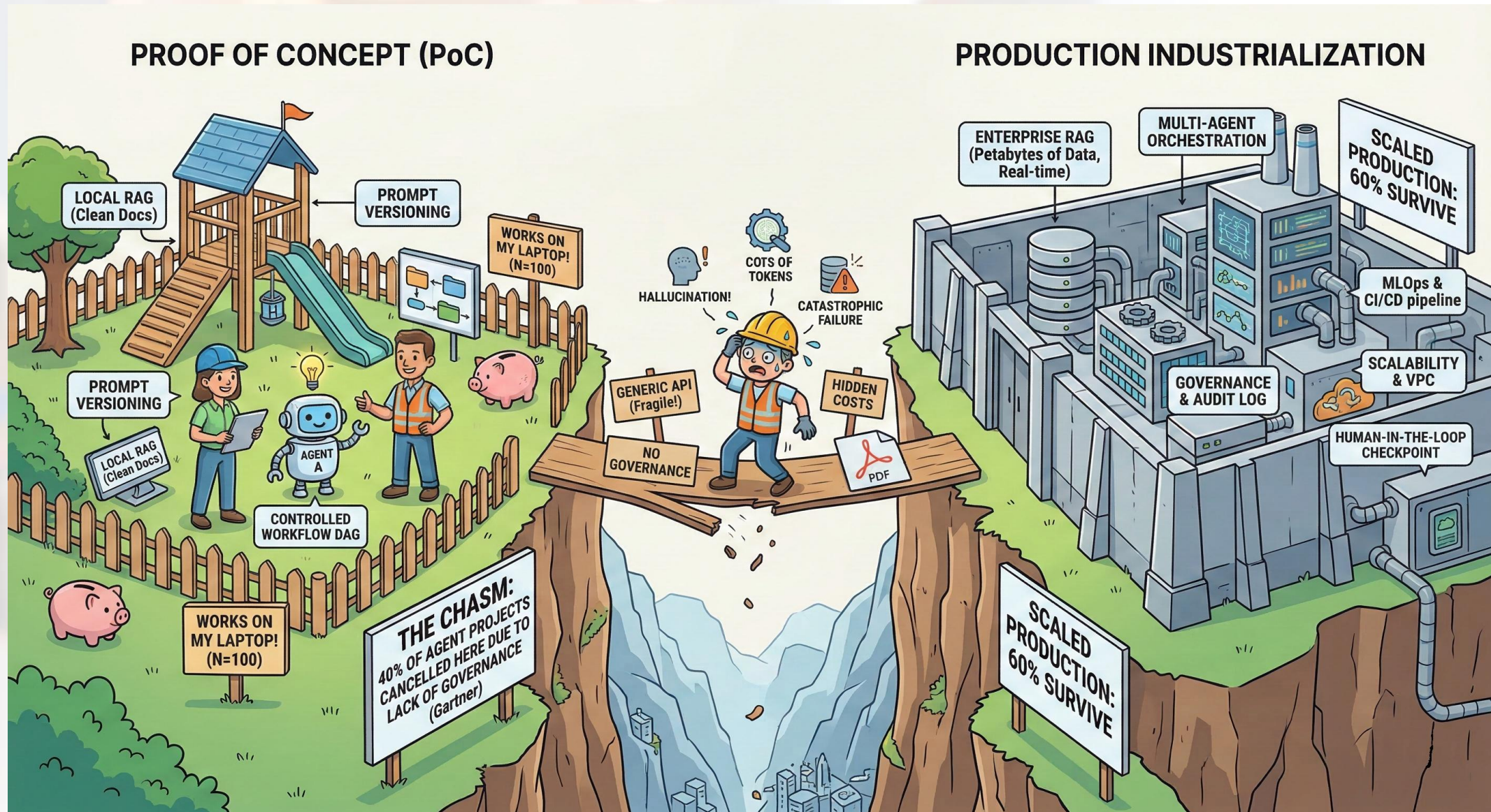


1. Generación de Valor: de la Tarea al Ecosistema



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

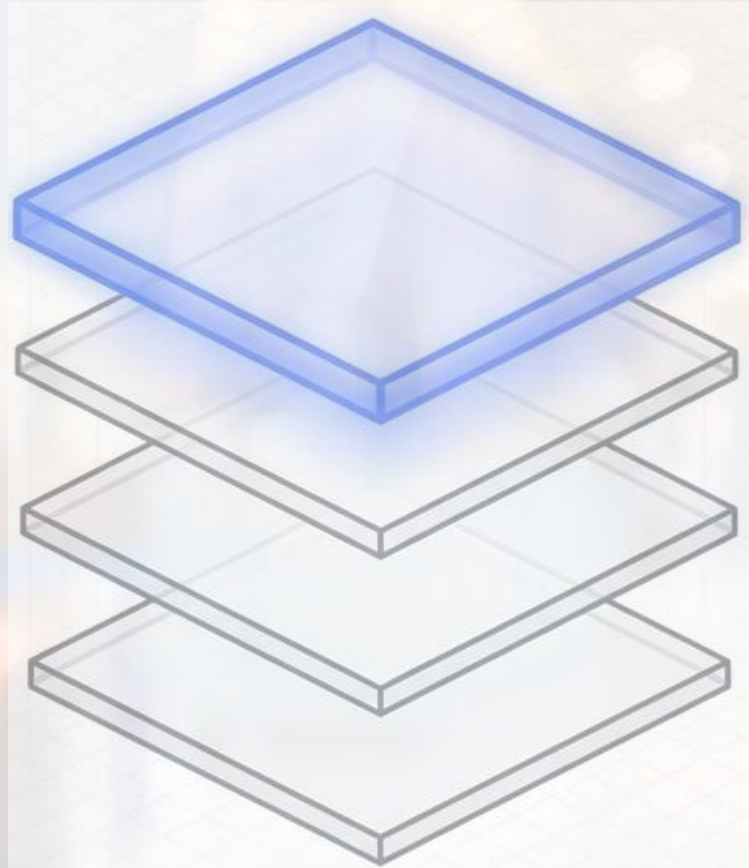
Consumo incontrolado de tokens o bucles infinitos de llamadas a herramientas pueden **disparar el TCO** drásticamente

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



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)



2. “Guardrails”

No dependen solo del modelo

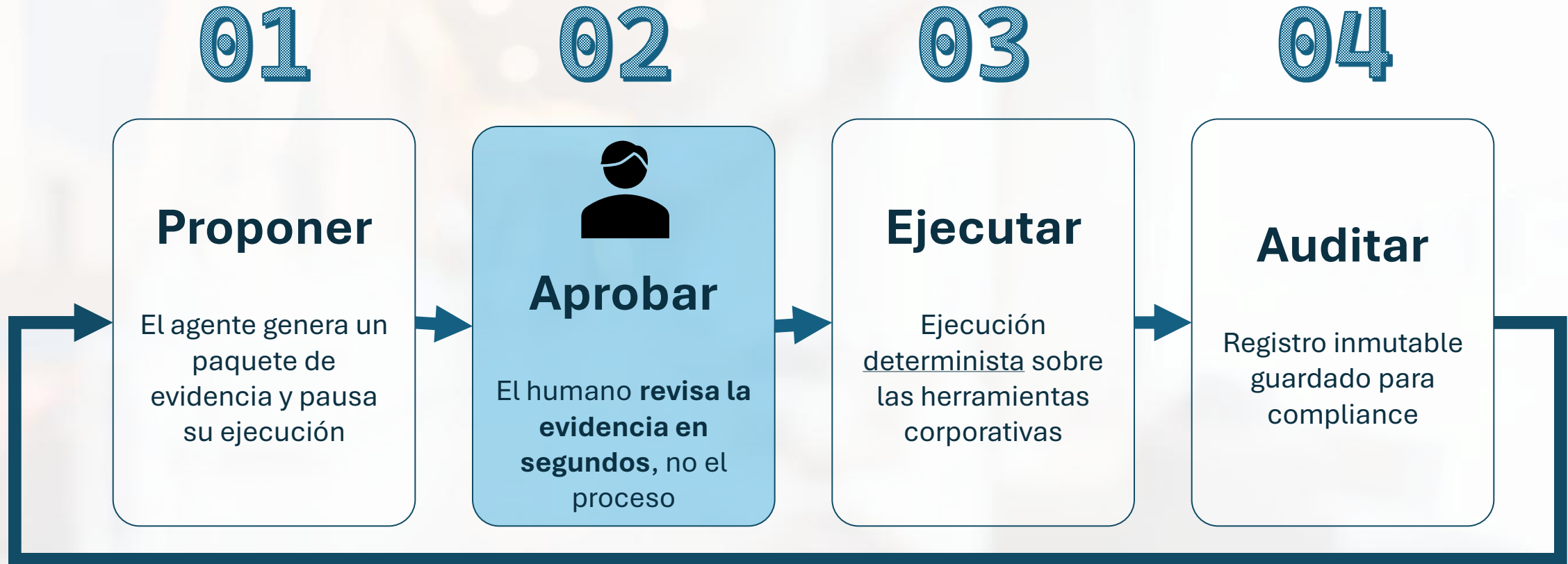
Da igual lo bueno que sea nuestro modelo, en un entorno determinado y con un contexto determinado, pueda acabar fuera de control



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



Alto impacto, alto alcance cognitivo



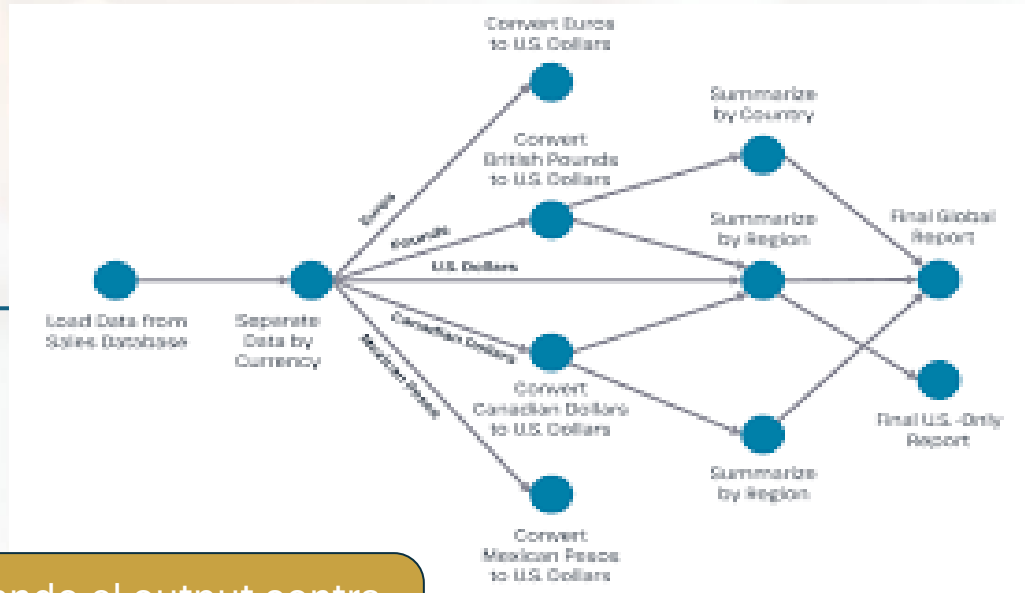
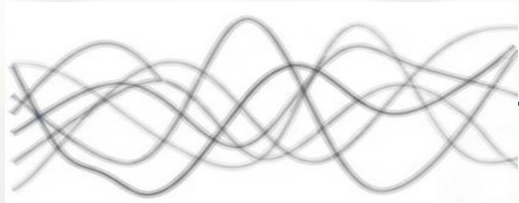
Separación arquitectónica estricta: autonomía máxima en el análisis / control absoluto en la acción

Problema: hay que evaluar bien qué metemos en el bucle, perdemos una parte de la eficiencia

2. “Guardrails” deterministas para entornos regulatorios

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

Conclusiones



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

01

Audit & Assessment

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



www.medallatech.com



contacto@medallatech.com