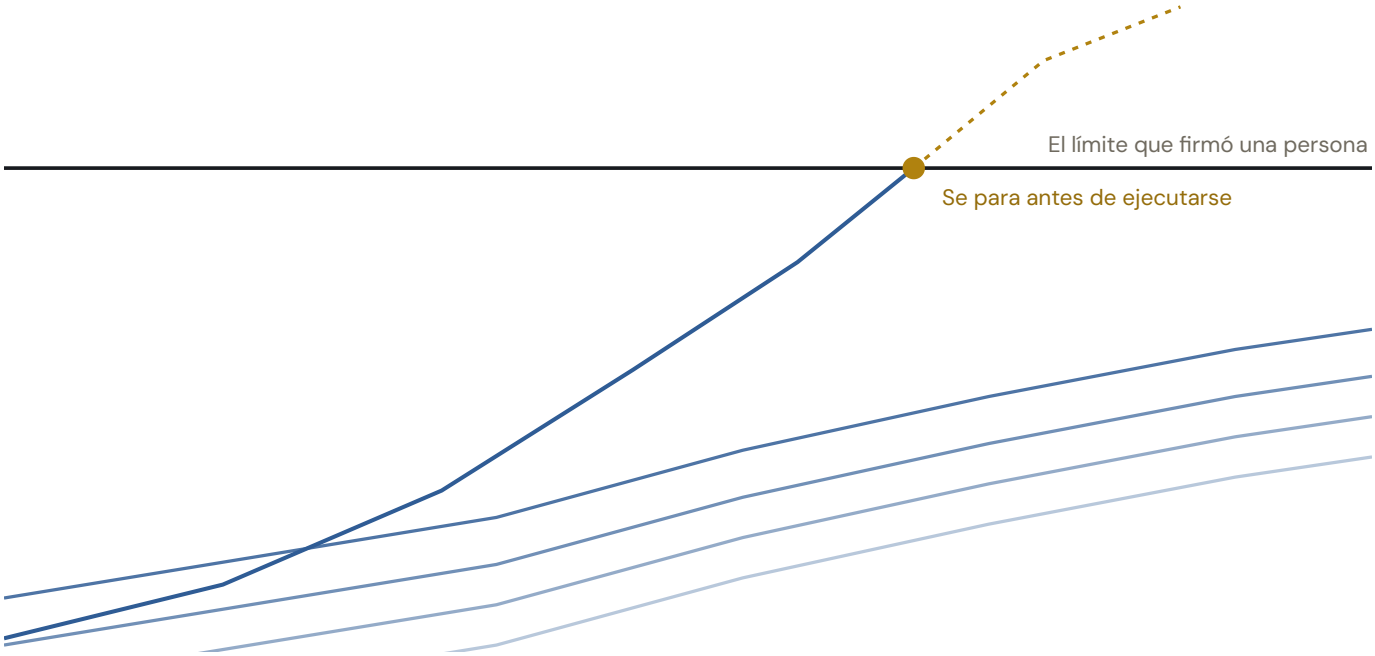
DiaCroma para Agentes (D4A)

Verit Global Labs

# Haz tu IA más segura.
# *Gestiona a tus agentes.*
# Y demuéstralo a tu auditor.



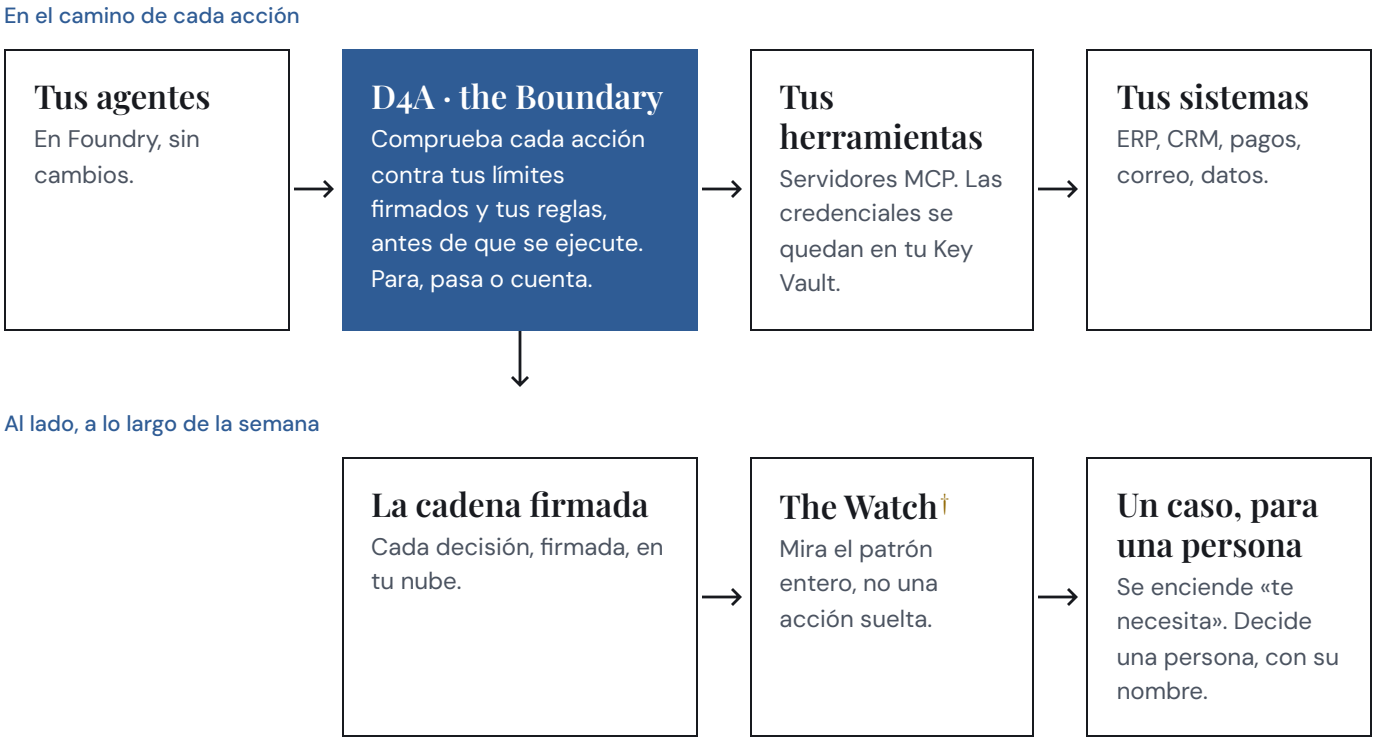

Tú decides los límites de tus agentes. **D4A comprueba cada acción, antes de que se ejecute.** Tu auditor recibe la prueba.

Pruébalo 30 días gratis en Microsoft Marketplace

marketplace.microsoft.com/en-us/product/veritglobal.d4a

# Para la acción equivocada. *Y detecta el patrón equivocado.*

Tú decides los límites de tus agentes. D4A comprueba cada acción.
Tu auditor recibe la prueba.




1 · The Boundary

## Para la acción equivocada, antes de que se ejecute.

Tus agentes tocan muchos sistemas. D4A comprueba cada acción una sola vez, en milisegundos, antes de que llegue a cualquiera de ellos. Si no pasa, nunca se ejecuta. No decide ninguna IA, y aunque nosotros caigamos, sigue haciendo cumplir.

2 · The Watch†

## Te avisa cuando un agente empieza a desviarse.

La deriva es silenciosa: cada acción está permitida, pero el agente hace su trabajo cada vez peor. D4A detecta la tendencia y abre un caso antes de que se convierta en un problema.

† en desarrollo

# Tus políticas están escritas. *Tus agentes no las leen.*

Sin nada que las haga cumplir, cada equipo pone sus reglas en un sitio distinto, y nadie ve si se cumplen ni cuál manda. **D4A las reúne y las hace cumplir en cada acción.** Muchos juegos de reglas, cada uno aplicado a su manera: D4A los aplica como uno solo.

| Tus reglas | Hoy | Con D4A |
|---|---|---|
| **Políticas de la empresa**<br>OPA, y Cedar† | Solo si un sistema pregunta. | Antes de cada acción, de cada agente. |
| **Guardarraíles de Foundry** | Solo si el agente obedece. | Firmados por una persona, aplicados desde fuera. |
| **Tus herramientas** | Lo que permita la credencial. | Solo las herramientas que alguien aprobó. |
| **Límites de negocio** | Nadie lleva el total. | Por operación y en total. Por día, cliente y equipo.† |

## Otras guardas que conservas

**Filtros de contenido de Foundry**
Déjalos al máximo.

**Presupuestos de Foundry**
Tokens y coste.

**Entra Agent ID**
Quién es cada agente.

**Tu jaula**
Donde corre el agente.

Si un agente está definido más flojo que las políticas de tu empresa, *mandan tus políticas.* Si no tienes políticas, mandan los límites del agente, firmados por una persona.

Tengas las reglas que tengas, cada agente queda cubierto. Como un seguro.

† en desarrollo

# Tus reglas de negocio pueden ser tan complejas *como tu negocio.*

Por operación, por día, por cliente, por equipo, todo a la vez. D4A las hace cumplir en cada agente, y suma lo que ningún agente ve por sí solo.†

## Diez agentes de descuentos, un presupuesto de equipo.†

| | |
|---|---|
| Cada agente | $100 por operación · $300 al día |
| El equipo | $500 al día |
| Cualquier cliente | $600 al mes |

A las 11:40 el equipo ya ha dado $400 hoy. Tres agentes piden $100 en el mismo segundo.

## $700

**Cada agente por su cuenta.** Todo sigue en verde: cada agente está dentro de sus límites. El equipo regala $200 de más.

## $500

**Con D4A.** Uno pasa, dos se paran. Decide el total del equipo, en un solo paso, así que tres agentes pidiendo en el mismo segundo no pueden pasar todos.

## Cada acción estaba permitida. *El total, no.*

Cifras ilustrativas. Hoy D4A lleva un total acumulado por agente, compartido por los agentes detrás de la misma Boundary; los totales por día, por cliente y por equipo están en desarrollo.

† en desarrollo

# The Watch te dice dónde mirar. *Tú decides.*†

Diez agentes hacen descuentos, cada uno dentro de sus límites. Y aun así uno de ellos ha dado el máximo al mismo cliente tres días seguidos.

| Lunes | Martes | Miércoles | Miércoles, 11:02 | Miércoles, 11:20 |
|---|---|---|---|---|
| Descuento máximo al cliente 4471. Permitido. | Máximo otra vez, mismo cliente. Permitido. | Máximo otra vez. Cada uno dentro de su límite. Permitido. | The Watch abre un caso con las acciones que forman el patrón. Se enciende «te necesita». | Una persona aprieta el límite, firmado con su nombre. |

Siempre activo y sin gastar tokens, the Watch ve la deriva que se acumula, agentes que se mueven a la vez y una misión que se deja de cumplir, con tus jueces de Microsoft en tu propio Azure.† Nunca para una acción ni cambia un límite: lo hace una persona.

# Una persona decide. *Tu auditor lo comprueba.*

## Autoriza a mano

Una acción parada se aprueba una vez, con firma y atada a esa acción exacta, y el agente la reintenta.†

## El caso, a quien firmó

Cada caso le llega a quien firmó el límite,† en la consola y también por Teams o por correo.†

## Cada uno con su rol

La autoridad firma los límites; el revisor lo lee todo y no puede cambiarlos. Ningún agente cambia sus propios límites.

## La prueba para tu auditor

Cada decisión queda en una cadena firmada, en tu nube. Tu auditor la verifica con una herramienta abierta, sin llamarte a ti ni a nosotros.† Demuestra que el registro no se alteró, no que el agente razonara bien.

† en desarrollo

# El gasto de tus agentes, *bajo control.*

Un agente tiene dos facturas: lo que hace con tu dinero, que llega de golpe, y los tokens, lo que gasta pensando, que crecen cada mes. D4A para lo primero y te avisa de lo segundo,† desde alrededor del 1 % de lo que ya te cuesta ejecutar tus agentes.

## Lo que hace con tu dinero

D4A lo para antes de que llegue a tu sistema. En producción, un reembolso de $10.000 contra un límite de $250 por llamada no se ejecutó.

| | |
|---|---|
| Ningún reembolso de más de $250. | Por llamada |
| No más de $2.000 en total. | Acumulado del agente |
| $600 por cliente al mes.† | Por periodo y cliente |

## El control de los tokens

El techo de tokens lo pone la plataforma que sirve el modelo (p. ej. Microsoft); D4A no lo duplica. Te dice lo que cuesta cada acción y corta lo que más quema sin que nadie lo vea.†

| | |
|---|---|
| Cuánto cuesta en tokens cada acción.† | Coste |
| Aviso a quien firmó el agente si sus tokens suben.† | Aviso |
| Corta los bucles: la misma llamada, una y otra vez.† | Bucles |

### Pagas por los agentes que gobiernas

Una cuota mensual fija. Las llamadas gobernadas son ilimitadas y nunca se miden.

### 30 días gratis

Cada plan empieza con 30 días gratis: cancela antes de que terminen y no se cobra nada.

### En Microsoft Marketplace

Con tu factura de Azure, sin llamada comercial. Para necesidades únicas, desde tu propia instalación, bajo acuerdo, y con el kit para partners.†

«You can’t have agents roam around and drift around the company.»

Jensen Huang, CEO de NVIDIA, en CNBC · 28 sep 2026

## Un agente no responde ante la ley. Tú sí. *Y además tienes que pagarlo.*

† en desarrollo

# D4A y la seguridad de agentes *que ya tienes.*

Hoy los agentes se protegen de tres maneras: un **gateway de IA** delante del modelo, un **gateway MCP** delante de las herramientas, o una **plataforma de seguridad de agentes**, que encuentra tus agentes y detecta amenazas. Cada una hace bien su trabajo, y D4A no sustituye a ninguna. Añade una cosa: antes de que una acción se ejecute, comprueba que cabe en lo que firmó una persona de tu negocio.

| | Gateway de IA | Gateway MCP | Plataforma de seguridad | Con D4A |
|---|---|---|---|---|
| **Lo que el agente hace con tu dinero** | Decide si el agente puede usar la herramienta de reembolsos | Decide si la herramienta está permitida para ese agente | Bloquea por herramienta, tipo de acción o destino | Decide si esta acción, con estos datos, cabe en lo que firmaste, y lleva la cuenta del total |
| **Quién pone las reglas** | Un administrador las configura | Un administrador las configura | El equipo de seguridad, o un asistente de IA | Las firma una persona del negocio, y quien revisa no puede cambiarlas |
| **La prueba para tu auditor** | Un registro que exportas y explicas tú | Un registro que exportas y explicas tú | Un registro que exportas y explicas tú | Una cadena firmada que tu auditor comprueba sin preguntar a nadie† |
| **Tus reglas de empresa** | Las vuelves a escribir en el gateway | Las vuelves a escribir en el gateway | Las vuelves a escribir en su consola | D4A le pregunta a tu OPA, o a Cedar†, antes de cada acción |
| **Lo que cambia con el tiempo** | Ve cada petición por separado | Vigila si cambia una herramienta | Compara al agente con su costumbre | Lo compara con lo que se le encargó† |

## Conserva lo que tienes. *D4A le añade lo que no ve.*

No hace falta que cambies tus agentes, tu gateway ni tu plataforma de seguridad. Si tienes cualquiera de los tres, D4A le añade valor; si no tienes ninguno, también funciona.

† en desarrollo

# Gobierna tu primer agente *esta semana.*

Plug and play. Los límites no se escriben desde cero: se leen de lo que ya les dijiste a tus agentes, y una persona los firma.

## Nada que cambiar en tus agentes, tus reglas ni tu negocio

Mismos agentes, mismas instrucciones, mismos modelos, mismas herramientas, y las reglas que ya tienes. D4A se coloca en el camino de cada acción desde la consola, que no escribe nada hasta que confirmas. Se puede deshacer.

## Empieza con cero riesgo

Sin coste: los primeros 30 días son gratis. Sin paradas: en Observing, D4A cuenta lo que habría parado y no bloquea nada. Después, tú eliges con qué dureza para:

**Observing** — Enforcing — Strict† — Explicit†

## Seis pantallas, sin código

1 **Store**
Consíguelo en Marketplace.

2 **Discover**
Encuentra tus agentes.

3 **Scan**
Propone límites, con su cita.

4 **Approve**
Tú firmas el mandato.

5 **Gateway**
Un contenedor en tu red.

6 **Health**
Gobernado o no, medido hoy.

## Habla con nosotros.

D4A está hoy en Microsoft Marketplace, para agentes en Microsoft Foundry. Otras plataformas vienen después.

diacroma@veritglobal.com
www.diacroma.com

† en desarrollo