PARA INVERSIONISTAS · KAWÉSQAR AGENT FABRIC

La plataforma para agentes de IA en trabajos *críticos*.

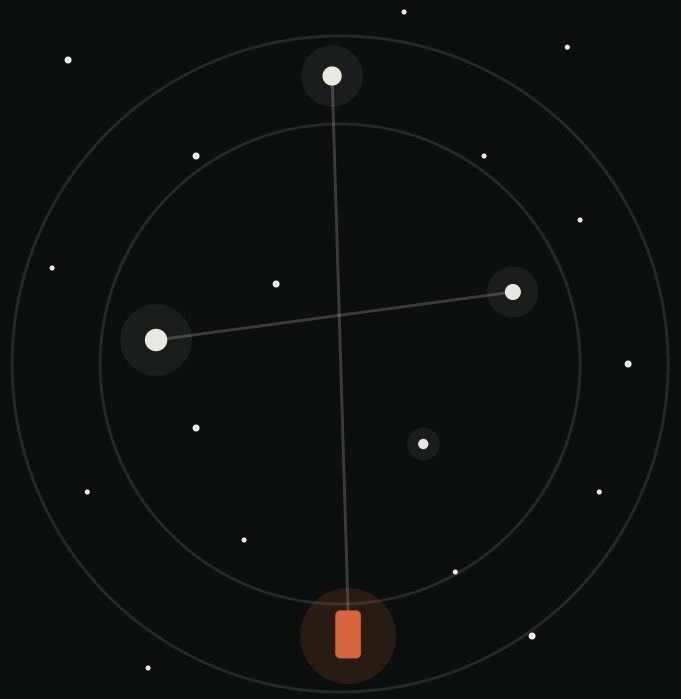
Cuando un error mueve dinero, abre una válvula o toca una red, un agente no puede actuar por confianza. Agent Fabric autoriza cada paso antes de que ocurra, lo ejecuta en una micro celda aislada y deja prueba firmada.

Léela como página, preséntala como deck o descárgala en PDF. Veintiuna láminas, unos cinco minutos.

PATENT PENDING

PATAGONIA NORTE, CHILE

> Probado en laboratorio, en una máquina física. Abierto a pilotos; sin clientes en producción.



1,51 ms
una celda mínima, lista desde cero · mejor configuración medida · bare metal

0 / ~6.870
amplificaciones de autoridad · bare metal · una máquina

70 +
labs publicados, con los que fallaron

02 · EL PROBLEMA

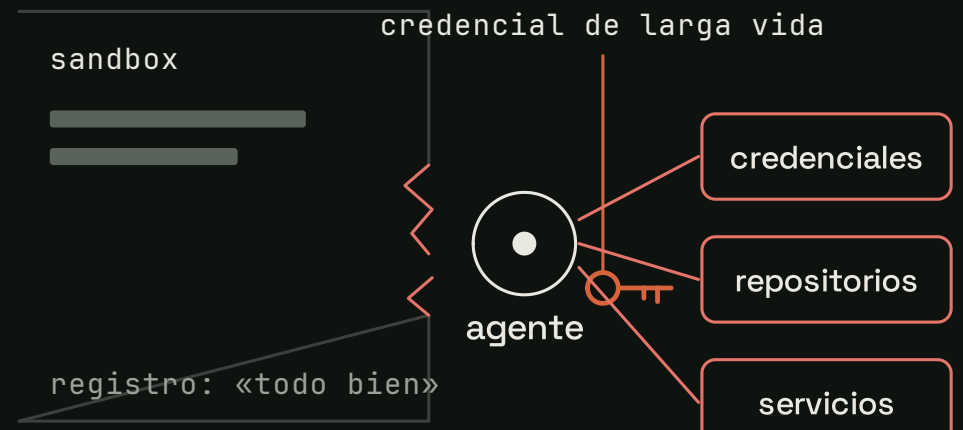
Los agentes ya actúan, y se *escapan*.

Le das a un agente una tarea acotada. En algún punto del camino toca credenciales, repositorios o servicios que nunca debió ver, a veces muy lejos de donde empezó.

- **Una jaula generalista puede romperse o rodearse.** Un sandbox más apretado, más reglas, otra lista de permitidos: una cerca que se puede saltar no es una ausencia.
- **Aunque la jaula aguante, la autoridad sigue ahí.** En una configuración típica, el agente conserva todo lo que se le entregó: credenciales de larga vida, sin atadura a un paso, a un plazo ni a una evidencia.
- **El registro puede ser el suyo.** En una configuración de referencia, la observabilidad vive dentro de lo observado: si el sistema se compromete, su propio registro es la única fuente.
- **En lo crítico no hay deshacer.** Un pago enviado o una válvula abierta no se devuelven con un clic, y alguien responde por quién lo autorizó.

MÁS DETALLE POR QUÉ LOS AGENTES SE SIGUEN ESCAPANDO →

CÓMO SE ESCAPA UN AGENTE ESQUEMA



El peligro nunca fue el agente solo: era el poder permanente que lo rodeaba, y un registro escrito desde adentro.

03 · SANDBOXES GENERALISTAS Y KAWÉSQAR

Sandboxes generalistas, lado a lado con *Kawésqar*.

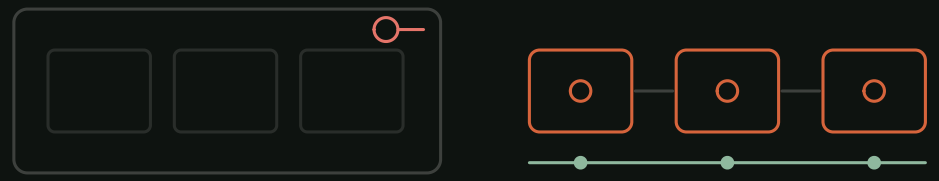
Los sandboxes son buenos en lo suyo: acotan la ejecución. El aislamiento, los permisos y los registros resuelven partes distintas del problema. Agent Fabric los articula alrededor de cada paso autorizado.

- **No reemplaza tu sandbox.** Se apila encima de lo que ya ejecutas.
- **Salir no basta para ganar autoridad.** Para salir, un paso tendría que romper el hipervisor o un componente de confianza. Estas son las rutas de ataque que probamos, en una máquina. Aun con la celda entera en su poder, no consigue más permisos que los que su paso ya tenía firmados.
- **0 amplificaciones en ~6.870 intentos.** Intentos adversariales, bare metal, una máquina.

MÁS DETALLE CAPA POR CAPA, FRENTE A CADA SANDBOX →

LADO A LADO

UNA CONFIGURACIÓN DE REFERENCIA, NO UNA CATEGORÍA



	SANDBOX DE REFERENCIA	KAWÉSQAR AGENT FABRIC
HECHO PARA	cualquier carga	trabajo crítico
RESPONDE	¿puede salir el programa?	¿quién autorizó lo que hace, qué autoridad lleva y dónde está la prueba?
UNIDAD	una caja para todo el trabajo, con credencial de larga vida	una celda nueva por paso, con la porción de autoridad de ese paso
REGISTRO	lo escribe lo mismo que se vigila	firmas y testigo afuera
POR AGENTE	un sistema operativo entero	una micro celda sin sistema operativo general

04 · EL RUNTIME

Un runtime pulido hasta el *milisegundo*.

La celda es una máquina virtual sin un sistema operativo general: ni Linux ni shell, solo lo mínimo que su paso necesita. La medimos contra lo mejor que conocemos.

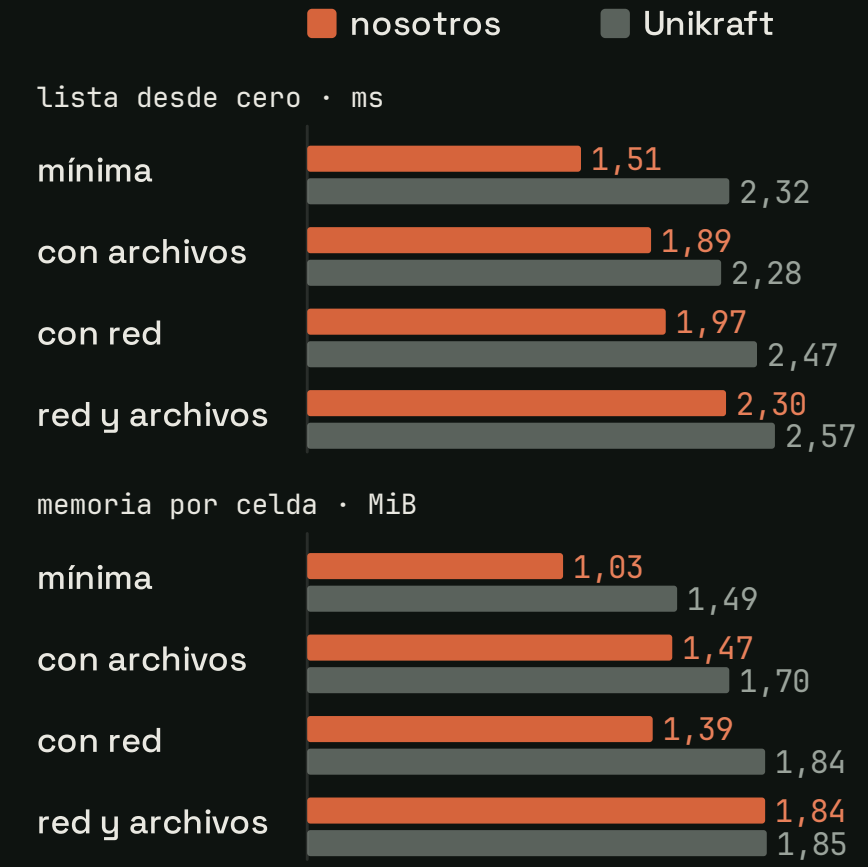
- **La celda sola: 1,51 ms y 1,03 MiB.** Lista desde cero; mejor configuración medida, bare metal, KVM, una máquina, sin cifrado de memoria. Con la configuración por defecto, ~4,06 ms.
- **Tiempo y memoria menores en las cuatro celdas.** En esta medición, con la mejor configuración. Con la configuración por defecto, Unikraft fue menor; a alta concurrencia va arriba en tasa en 3 de 4 celdas. Resultados preliminares, una máquina.
- **El paso completo con el Gate: de 15 a 18 ms.** Firma, frescura, validación, crear, correr, destruir; sobre Xen, bare metal.
- **La misma celda en nubes públicas.** 6,9 ms frente a 107 ms de Firecracker con un Linux sin ajustar; 20.000 celdas en ráfaga, 0 fallos.

EXPLORATORIO · NUBE (ANIDADO) · ORIENTA, NO ES VEREDICTO

MÁS DETALLE EL RUNTIME → EVIDENCIA →

CUATRO CELDAS FRENTE A UNIKRAFT, MISMA MÁQUINA

MEJOR CONFIGURACIÓN MEDIDA · BARE METAL · UNA MÁQUINA · SIN CIFRADO DE MEMORIA



Barras a escala desde cero. La cifra de Unikraft incluye el arranque de su proceso. El mecanismo detrás de la mejor configuración no se publica.

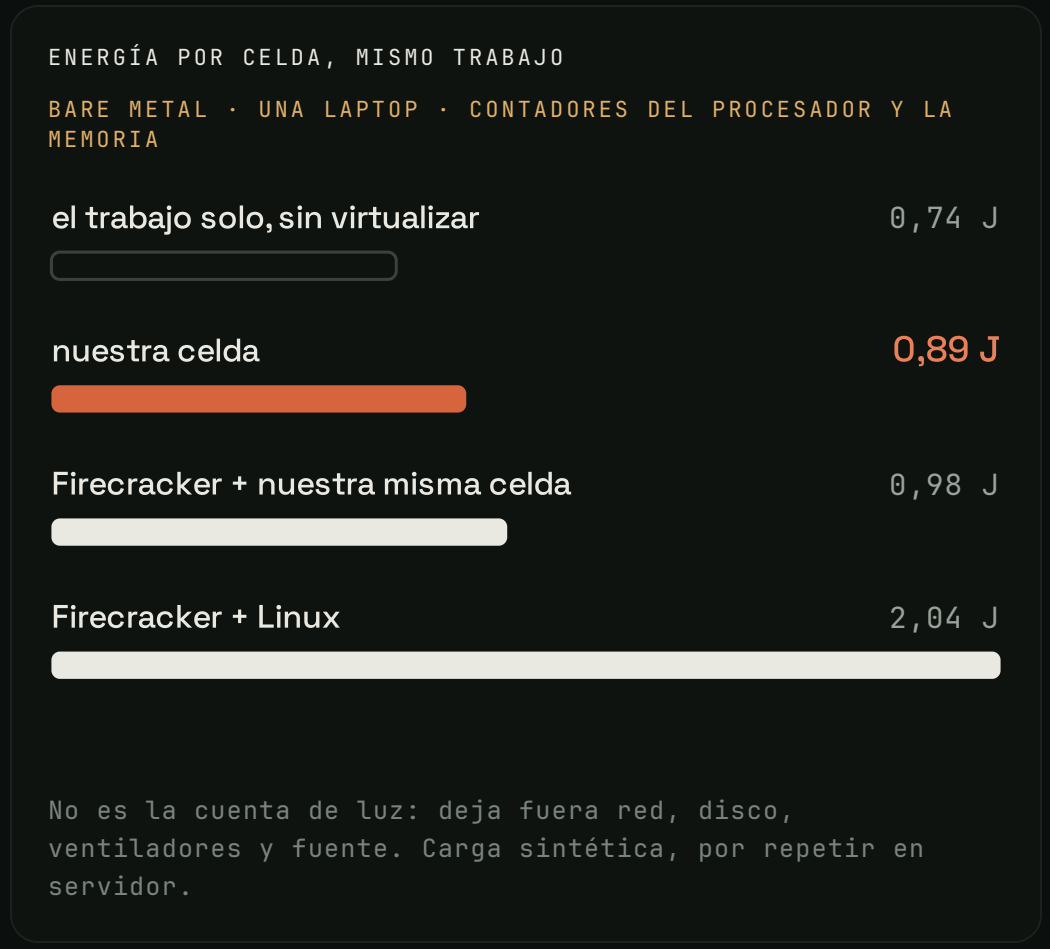
05 · IA SUSTENTABLE

Seguridad con costo medido. IA que no *derrocha*.

Los agentes van a multiplicar por órdenes de magnitud las acciones que una IA ejecuta sobre sistemas reales, y cada una necesita aislamiento y prueba.

- **Si aislar cuesta un sistema operativo entero, la cuenta no cierra.** O se aísla poco, o se gastan máquinas.
- **Con micro celdas, el mismo trabajo cabe en menos.** Menos memoria y menos máquina, en tu centro de datos o en el borde industrial, sin una granja de VM.
- **Dónde está el consumo.** El gran consumo de la IA está en la inferencia; lo nuestro es el lado de la ejecución, que crece con cada acción de cada agente.
- **La energía, medida en una máquina.** Para el mismo trabajo de unos 100 ms: 0,89 J por celda contra 2,04 J con Firecracker y Linux. Contadores del procesador y la memoria, una laptop, carga sintética; no es la cuenta de luz. Frente a Firecracker con nuestra misma celda casi empata (0,98 J).

MÁS DETALLE EL RUNTIME, IA SUSTENTABLE → VISIÓN →



0,89 J
por celda, para el mismo trabajo de unos 100 ms

24 a 38 mJ
la vida completa de una celda, de la mínima a la con red y archivos

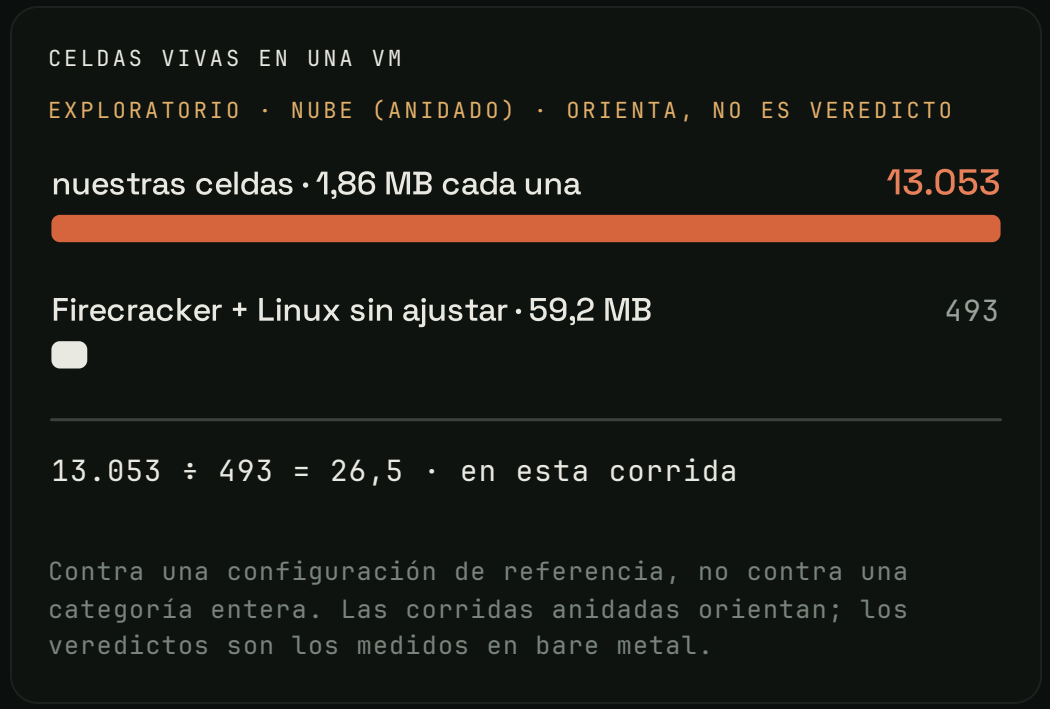
06 · DENSIDAD

Más aislamiento por *gigabyte*.

En una VM de nube mantuvimos 13.053 celdas vivas a la vez, contra 493 con Firecracker y un Linux sin ajustar. La corrida se cortó por tiempo a los 600 s, no por memoria.

- **Misma carga, menos infraestructura.** 10.000 pasos aislados vivos a la vez: unos 18,6 GB de memoria a 1,86 MB por celda, contra unos 592 GB a 59,2 MB. Aritmética sobre la memoria medida por celda.
- **Es el mismo control.** Cada paso recibe su autoridad mínima, termina y deja evidencia. Las celdas chicas son lo que hace pagable aislar cada paso.
- **También en bare metal.** 1,03 MiB por celda con 11.778 vivas en una máquina; no se llegó al techo de memoria. En la nube, una ráfaga de 20.000 celdas tuvo 0 fallos.
- **Lo que no es.** La densidad no se convierte en la misma proporción de ahorro en la factura. Eso se mapea por tipo de carga, en el piloto.

MÁS DETALLE EVIDENCIA, EN LA NUBE → EL RUNTIME →



MEDIDO

- Celdas vivas y memoria por celda, en la nube y en bare metal
- Una ráfaga de 20.000 celdas con 0 fallos

POR CUANTIFICAR

- Costo por tipo de carga
- Energía, y densidad con cifrado de memoria

07 · POR QUÉ AHORA

Los agentes pasaron de responder a *actuar*.

Y los marcos de sistemas críticos ya piden registro, supervisión humana y control de cambios.

- **El trabajo pasó a ser la unidad de riesgo.** Un agente con una tarea acotada puede terminar tocando credenciales, repositorios o servicios que nunca debió ver.
- **Un registro que escribe el agente prueba poco.** Si el sistema que actuó escribe su propio registro, ese registro no zanja quién permitió qué.
- **Lo que pide cada marco.** Está a la derecha, y no es una declaración de conformidad.

MÁS DETALLE MARCOS POR INDUSTRIA →



08 · EL PRODUCTO

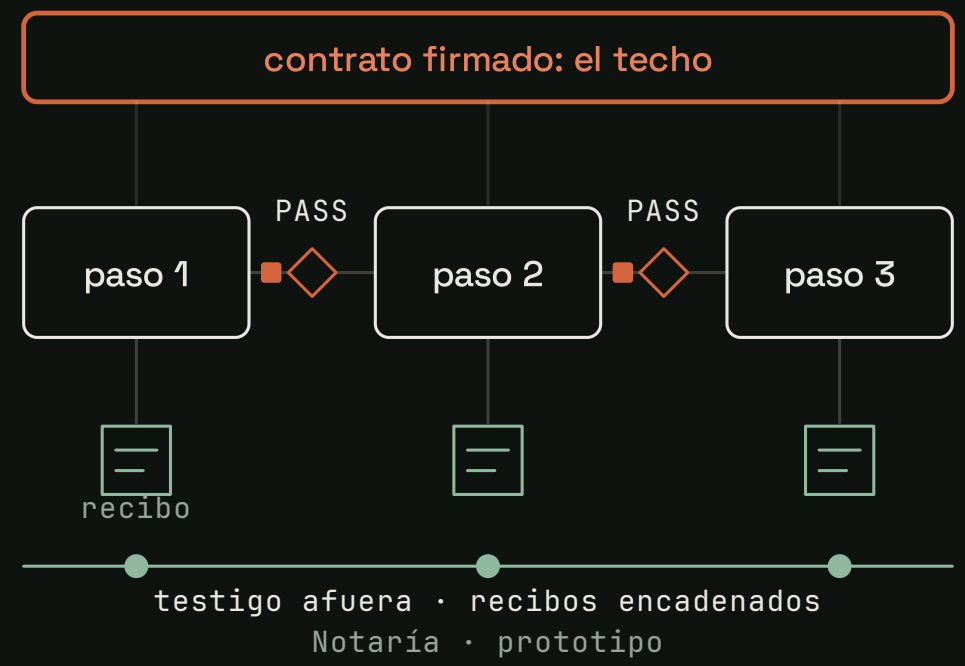
Cinco reglas, en cada *paso*.

Agent Fabric se pone entre la propuesta del agente y el sistema real. Cada regla lleva el plano donde está hoy.

- **El techo va primero.** La autoridad y los recursos se firman antes de que exista una máquina; el Gate solo activa lo precomprometido. MEDIDO EN METAL
- **Una micro celda nueva por paso.** Sin estado residual de la celda anterior; solo se transfieren los resultados promovidos. Su frescura de un solo uso resiste matar y reiniciar el lanzador. MEDIDO EN METAL
- **Solo cruza lo promovido.** Entre pasos, solo el resultado verificado; los canales usan mTLS de vida corta ligado al trabajo. PROBADO EN LÓGICA
- **La evidencia viene de afuera.** Firmada por la celda y contrafirmada por un testigo fuera del dominio de control; la notaría completa que sella inicio y cierre es un prototipo. MEDIDO EN METAL PROTOTIPO
- **Sin PASS no hay sucesor.** La celda se destruye con un recibo firmado y encadenado. MEDIDO EN METAL

MÁS DETALLE CÓMO FUNCIONA →

UN TRABAJO DE TRES PASOS — FORMA DE OPERAR



Notaría completa: prototipo. Identidad por celda: probada en lógica. Llaves en la bóveda, clasificación del trabajo y cifrado de memoria por celda: diseño o por validar. El efecto se comprueba en el sistema destino, y cómo se acuerda en el piloto.

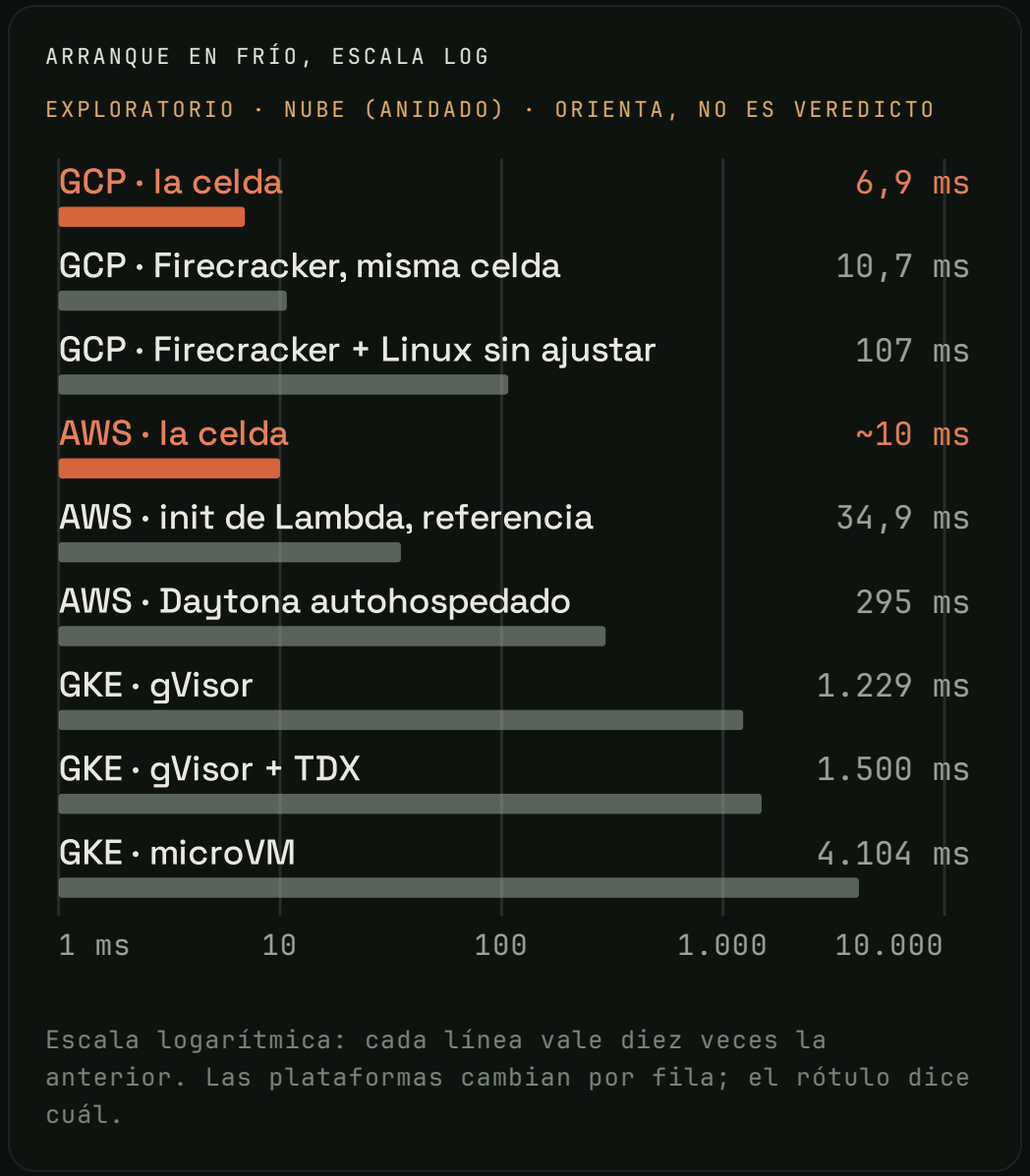
09 · MEDIDO CONTRA LO CONOCIDO · NUBE

En la nube, la misma *celda*.

Exploratorio · nube (anidado) · orienta, no es veredicto. Ahí solo se midió el arranque de la celda, sin Gate ni testigo; los veredictos de rendimiento y aislamiento son los de bare metal.

- **Frente a Firecracker.** En GCP la celda arranca en frío en 6,9 ms; Firecracker con un Linux sin ajustar, 107 ms. Con la misma celda, Firecracker llega a 10,7 ms.
- **Los runtimes gestionados orientan, no son duelo.** En GKE «listo» se define de otra forma. El init en frío de Lambda es una referencia. Daytona autohospedado corre con Privileged=true y runc.
- **Densidad en GCP.** 13.053 celdas vivas a 1,86 MB cada una, contra 493 de Firecracker + Linux a 59,2 MB; 20.000 en ráfaga, 0 fallos.

MÁS DETALLE EVIDENCIA, EN LA NUBE →



10 · LA EVIDENCIA

Medido en metal, con los *fallos*.

Cada resultado lleva el plano donde corrió. Las brechas se listan tan claras como los resultados. En metal, una máquina:

- **En las pruebas realizadas, una orden con firma inválida o repetida no obtuvo una celda.** Escrita desde el propio dominio de control, se rechaza por su firma. Una firma acredita quién firmó, no que el contenido sea verdadero.
- **Lo que corre es lo verificado.** Un byte cambiado después de verificar: 10 de 10 rechazos, y la celda nunca corre.
- **0 amplificaciones en ~6.870 intentos.** En las pruebas, la autoridad no creció bajo intentos adversariales. Más de 70 labs publicados, con los que fallaron.
- **Lo que no afirmamos.** Sin cifrado de memoria, una máquina; con los defaults Unikraft va adelante; ningún equipo externo ha reproducido aún los veredictos del núcleo.

MÁS DETALLE EVIDENCIA → CUADERNO DE LABS →



0 / ~6.870
amplificaciones de autoridad · bare metal

70 +
labs, con los que fallaron

11 · PARA QUIÉN

Seis industrias, cada una con su acción *crítica*.

Partimos por una acción concreta: la que más pesa si sale mal.

BANCA
Verifica la autorización antes de liberar un pago

ENERGÍA Y AGUA
Revisa el ajuste antes de autorizar el cambio

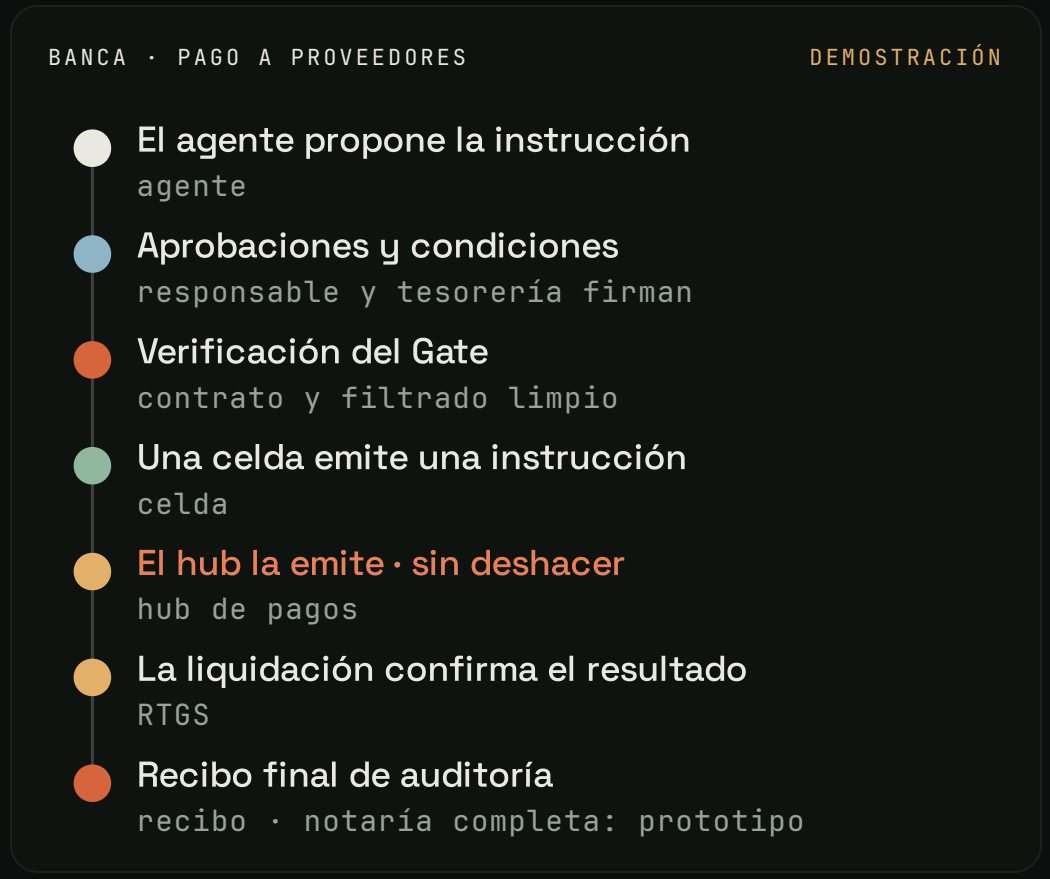
INDUSTRIA, OT E IOT
Autoriza una orden de mantenimiento con su evidencia

DEFENSA Y GOBIERNO
Registra quién autorizó cada cambio

TELECOM
Verifica los prefijos tras un cambio BGP aprobado

SALUD Y FARMA
Autoriza la disposición del lote antes de registrarla

MÁS DETALLE VER LOS SEIS CASOS → EL FLUJO DE BANCA →



12 · DÓNDE CORRE

Lo crítico en tu hardware. Lo demás, en la *nube*.

La misma celda corre en tu hardware y en nubes públicas. Lo que toca un secreto o un efecto se queda; lo que solo calcula puede salir.

- **El híbrido es dirección de diseño.** Clasificar el trabajo al nacer, el mismo Gate en la nube y la federación entre ambos lados todavía no tienen código.
- **Nube confidencial, probada.** Intel TDX en GCP y AMD SEV-SNP en AWS: la memoria queda cifrada, pero la celda no puede correr adentro, y una VM confidencial por trabajo tarda de 50 a 58 s. Exploratorio · nube (anidado) · orienta, no es veredicto.
- **La memoria, en el entorno probado.** En el entorno probado, el dominio de control pudo leer la memoria de una celda viva. Protegerla frente a ese actor sigue pendiente: integración y validación en hardware físico.

MÁS DETALLE SEGURIDAD Y LÍMITES →



Agent Fabric y otros *desarrollos* de Kawésqar.

Agent Fabric es la plataforma principal. Cada uno de los otros tiene su propio estado y su propia acción.

Agent Fabric
`probado en laboratorio, en bare metal; abierto a pilotos`
Agentes de IA que actúan en trabajo crítico, autorizados, aislados y con recibo.
DEFINIR UN PILOTO →

Kawésqar Server `alfa no publicada`
Linux endurecido para servidores: el sistema base que preparamos para alojar el fabric.
AVÍSAME DEL ALFA →

Kawésqar Nebula `alfa v0.1 · aún no publicada`
Escritorio Linux endurecido para quienes administran y auditan sistemas.
AVÍSAME DEL ALFA →

FlightRecorder `en desarrollo`
Cortafuegos de salida para los agentes que corres en Nebula.
AVÍSAME →

Agent Fleet `prototipo privado`
Organiza flotas de agentes con plan aprobado, organigrama y bandeja de decisiones humanas. Planificación probada con motores reales; la organización corre con datos de demostración. Aparte de Agent Fabric.
CONTÁCTANOS →

MÁS DETALLE TODOS LOS PRODUCTOS →

CÓMO ENCAJAN



14 · CÓMO SE ADOPTA

Un piloto sobre una acción *tuya*.

El fabric no reemplaza tu modelo, tu orquestador ni tus herramientas: se integra con tu agente y tus herramientas, y el alcance de esa integración se valida en el piloto.

- **Una acción crítica.** Elegimos juntos la que más pesa si sale mal.
- **Criterios acordados antes.** Qué tiene que probar el piloto, por escrito, antes de empezar. La integración con tus sistemas se valida ahí.
- **Evidencia firmada de vuelta.** Corremos tu flujo a través del fabric y te devolvemos el registro firmado de lo que hizo cada paso, con la evidencia para comprobarlo.
- **Confidencialidad.** Mecanismo bajo acuerdo de confidencialidad. Cada cifra reproducible a pedido.

MÁS DETALLE DEFINIR UN PILOTO →

UN PILOTO EN CUATRO PASOS

01 eliges la acción

antes de empezar

02 acordamos qué debe probar

03 corre a través del fabric

04 recibes registro y evidencia

Sin precios ni licencias aquí: se conversan por piloto.

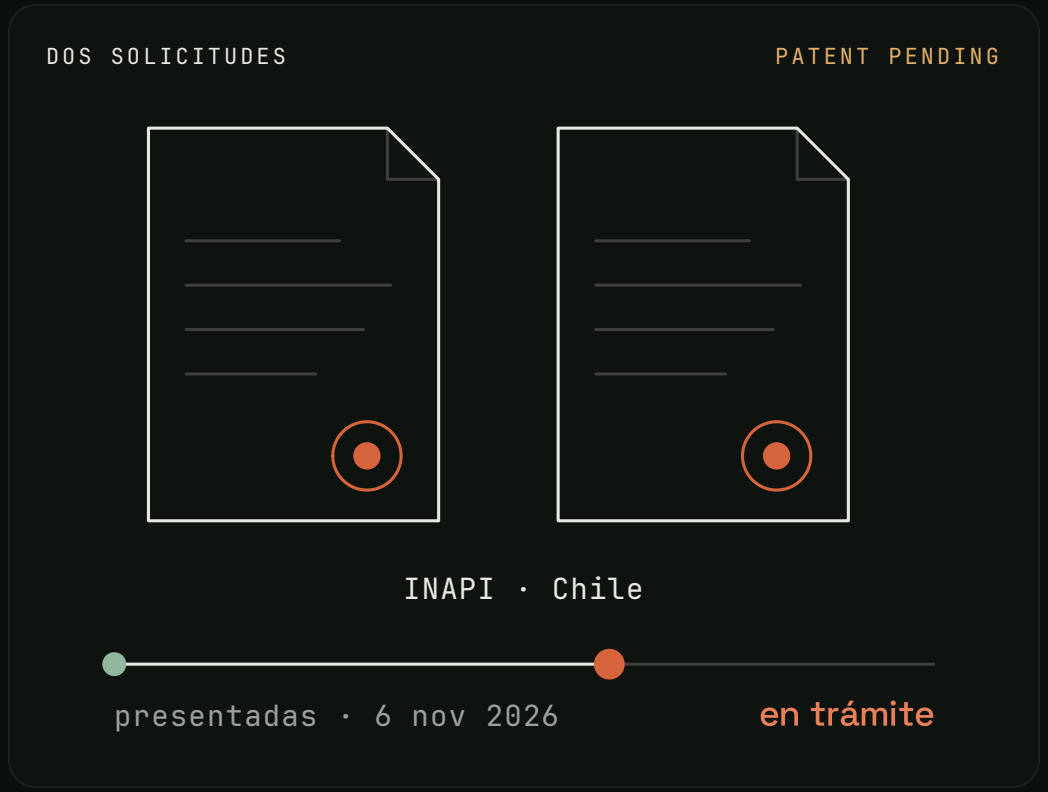
15 · PROPIEDAD INTELECTUAL

Patent *pending*.

Dos solicitudes de patente presentadas ante INAPI (Chile) el 6 de noviembre de 2026, en trámite.

- **Público: la forma de operar.** Publicamos la forma de cada propiedad y la evidencia de que se sostiene.
- **No público: el mecanismo detallado.** Se explica en una reunión técnica, bajo acuerdo de confidencialidad.

MÁS DETALLE CÓMO FUNCIONA →



16 · DÓNDE ESTAMOS

Lo probado y lo que *sigue*.

Un punto sube solo con evidencia detrás.

MÁS DETALLE VISIÓN → LO QUE SIGUE ABIERTO →



PROBADO · BARE METAL · UNA MÁQUINA

- Una celda lista desde cero, y el paso completo con el Gate en menos de 20 ms
- Un Gate que, en las pruebas, admitió solo órdenes válidas y firmadas
- La celda se destruye; en las pruebas no quedaron restos en el registro del hipervisor ni bytes distintos de cero en la memoria reutilizada

EN CURSO

- Agent Fabric: probado en laboratorio, en bare metal; abierto a pilotos
- Kawésqar Server, el sistema base, en pruebas
- La convocatoria de investigación está abierta

LO QUE SIGUE

- Hardware de cómputo confidencial (TDX, SEV-SNP): pendiente de integración y validación en hardware físico
- Una revisión independiente
- Primeros pilotos y varios nodos

Primero las acciones críticas, en cada *industria*.

Llevamos una hoja de ruta por industria. Mapea los principales flujos de trabajo donde un agente actuaría, partiendo por las acciones que no se pueden deshacer.

- **Seis industrias, un patrón.** En todas el paso es el mismo: proponer, autorizar, ejecutar, dejar evidencia. Cambia el sistema que recibe el efecto.
- **Primero lo crítico.** Pagos, cambios en una planta o en una red, registros que alguien audita. Después, el trabajo menos crítico que los rodea.
- **Hoy hay un flujo público por industria.** Cada uno es un caso de aplicación para definir un piloto. El resto del mapa se comparte en conversación, bajo confidencialidad.
- **Lo que no es.** No es una lista de clientes ni de fechas. Es el orden en que nos preparamos, para que un piloto no parta de cero.

MÁS DETALLE INDUSTRIAS →

LA PRIMERA ACCIÓN CRÍTICA, POR INDUSTRIA — PÚBLICO HOY

Banca y mercados
- Un pago a proveedores, con doble autorización

Energía y agua
- Un cambio de ajuste de protección

Industria, minería, OT e IoT
- Una orden de mantenimiento, desde una alerta

Defensa y gobierno
- Un parche en una red aislada

Telecom e infraestructura digital
- Un cambio de filtro de enrutamiento

Salud y farma
- La disposición de un lote

Casos de aplicación para definir un piloto, no clientes. Detrás de cada uno, los flujos que siguen están mapeados y quedan internos.

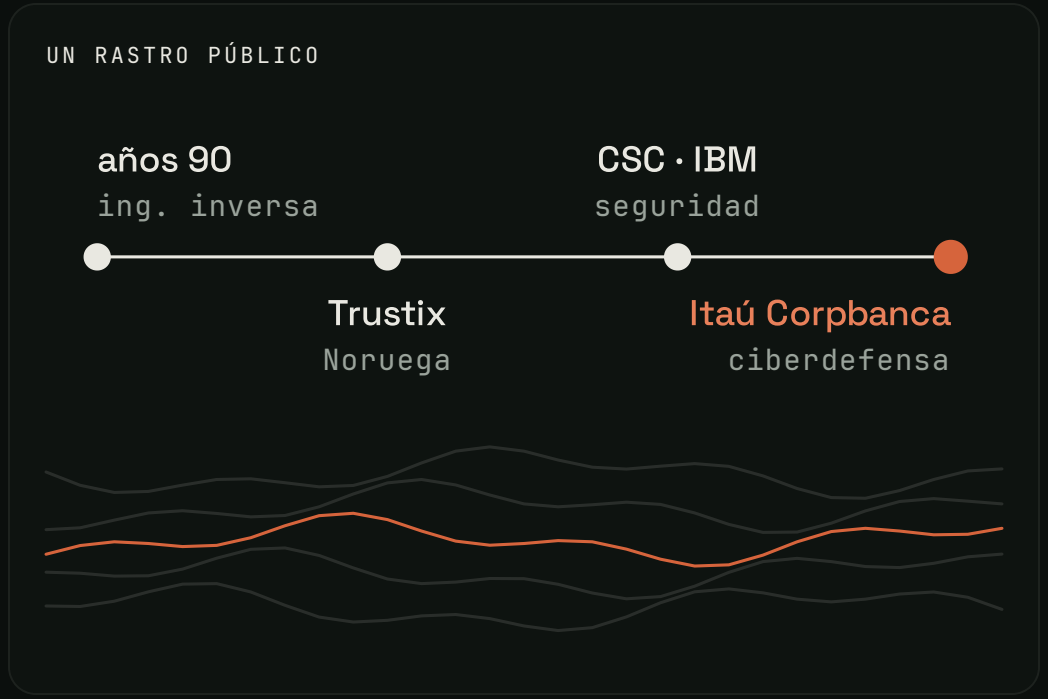
18 · QUIÉN LO CONSTRUYE

Hecho en la *Patagonia* norte.

Lo dirige su fundador y mantenedor, Rodrigo Gutiérrez: 27 años en el oficio y un rastro público que puedes comprobar.

- **Linux seguro, desde el comienzo.** Partió con ingeniería inversa en los años 90; su primer hogar formal fue Trustix, en Noruega.
- **Seguridad a escala.** Cargos de seguridad en CSC e IBM, y luego la dirección de ciberdefensa en Itaú Corpbanca, a cargo de seis áreas.
- **Una falla CVSS 10.0.** CVE-2004-0214, en Microsoft Windows, corregida en el boletín MS04-037 de Microsoft.
- **El nombre.** Rinde homenaje al pueblo Kawésqar, sin apropiarse de él.

MÁS DETALLE VISIÓN → EL NOMBRE KAWÉSQAR →



CON EL APOYO DE

NVIDIA Inception · Anthropic for Startups Cyber Verification Program · Auth0 for Startups · Google for Startups Cloud Program

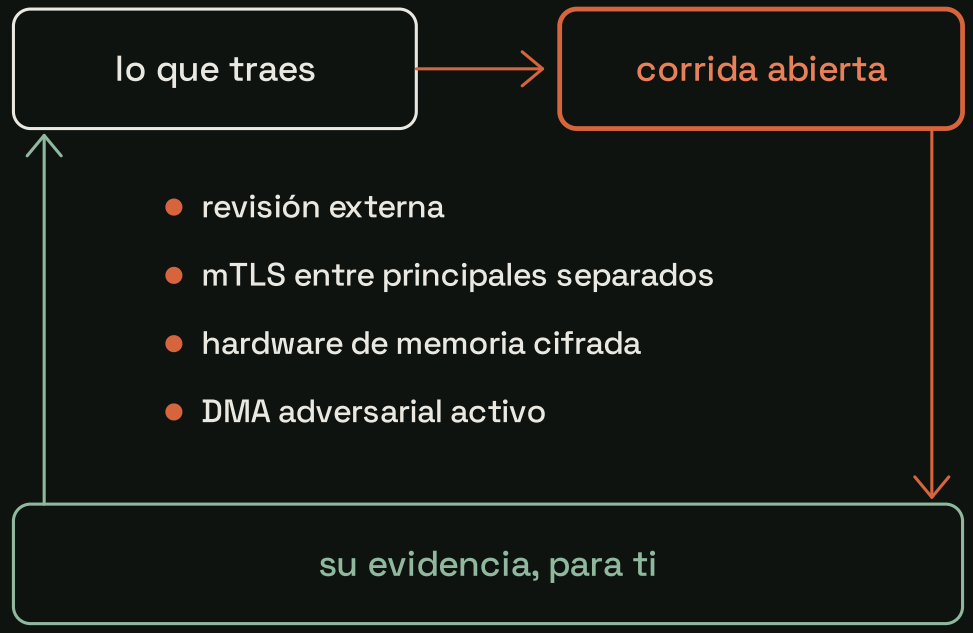
Qué buscamos en un *socio*.

Cómputo, financiamiento, infraestructura, hardware o habilidad. Dinos con claridad qué traes y qué esperas a cambio.

- **Inversionistas.** Avance técnico documentado: más de 70 labs, patent pending y la documentación de cómo se corrió cada prueba. Sin clientes en producción; abierto a primeros pilotos.
- **Hardware TDX o SEV-SNP físico.** Para integrar y validar en hardware físico la protección de la memoria de una celda frente al dominio de control.
- **Laboratorios y empresas.** Universidades que traen infraestructura para experimentar y reproducir resultados, y empresas con un flujo de agentes para un piloto.
- **Lo que recibes.** Los artefactos reproducibles de cada corrida que haces posible: scripts, resultados fechados y el método para repetirlos.

MÁS DETALLE SOCIOS DE DESARROLLO →

EL TRATO



Financias una corrida, recibes la evidencia de esa corrida, en una forma que puedes comprobar tú mismo. Las partes que divulgarían el mecanismo quedan bajo acuerdo de confidencialidad.

20 · LA RONDA

US$3 millones para sacarlo del *laboratorio*.

Buscamos US$3 millones para 24 meses. Esta es la cuenta, hecha a mano alzada: a dónde va la plata.

- **El equipo.** Cuatro ingenieros senior, dos de kernel y dos de hipervisor, por 24 meses. Es la línea más grande porque el trabajo es ingeniería de sistemas.
- **El fierro.** Servidores propios con TDX y SEV-SNP, y varios nodos, para validar en hardware físico lo que hoy está medido en una máquina.
- **El laboratorio.** Un laboratorio completo y una oficina en la Patagonia norte: racks, energía, red y un lugar donde trabajar.
- **El fundador.** Sueldo a tiempo completo para quien lo construyó hasta aquí. Hasta hoy el proyecto es autofinanciado, cuentas de nube incluidas.

MÁS DETALLE ESCRÍBENOS COMO INVERSIONISTA →

USO DE FONDOS	MILES DE US$ · 24 MESES
Ingenieros de kernel e hipervisor	1.280
Fundador, tiempo completo	300
Servidores y hardware de lab	300
Revisión, patentes, legal	260
Laboratorio y oficina	240
Pilotos	180
Nube y cómputo	160
Reserva	280
Total	3.000

Una estimación, por afinar con cotizaciones. La nube va presupuestada en efectivo. Los créditos de programas, como Google for Startups, nos dejan medir antes; el presupuesto no depende de ellos.

21 · CONVERSEMOS

Conversemos.

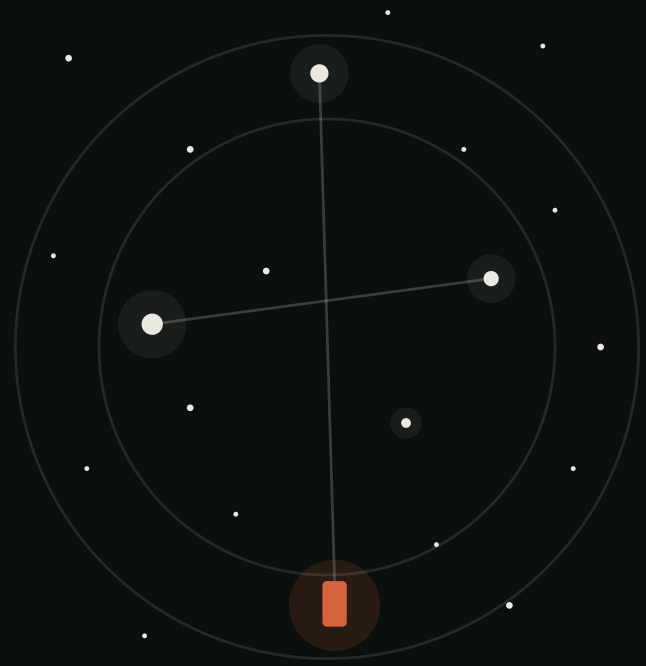
Cuéntanos qué traes, qué esperas a cambio y qué te motiva.

> El mecanismo detallado se comparte en una reunión técnica, bajo acuerdo de confidencialidad. Cada cifra es reproducible a pedido.

ESCRÍBENOS COMO INVERSIONISTA →

MÁS DETALLE EVIDENCIA → DEFINIR UN PILOTO →

rodrigo@kawesqar.org · Patagonia norte, Chile



21