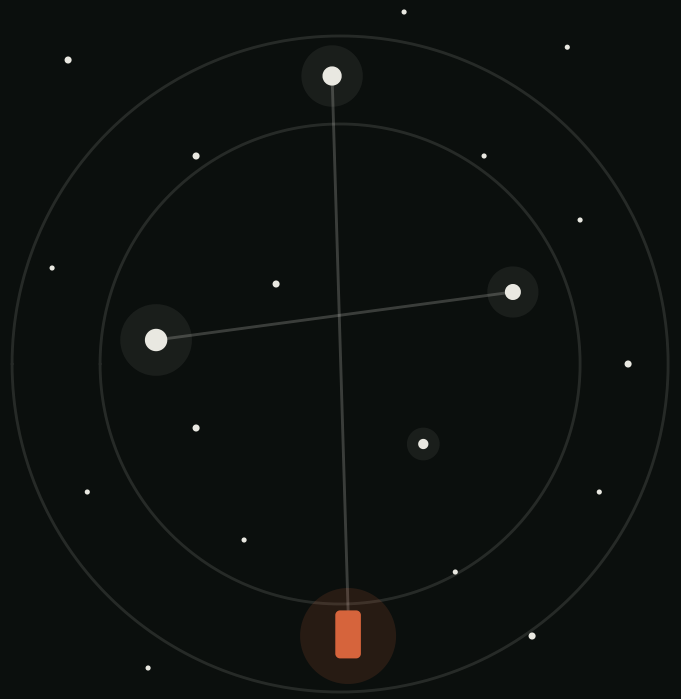
PARA INVESTIDORES · KAWÉSQAR AGENT FABRIC

A plataforma para agentes de IA em trabalhos *críticos*.



Quando um erro move dinheiro, abre uma válvula ou toca uma rede, um agente não pode agir por confiança. O Agent Fabric autoriza cada passo antes que aconteça, executa numa microcélula isolada e deixa prova assinada.

Leia como página, apresente como deck ou baixe em PDF. Vinte e uma lâminas, uns cinco minutos.

PATENT PENDING | PATAGÔNIA NORTE, CHILE

> Testado em laboratório, em uma máquina física. Aberto a pilotos; sem clientes em produção.

1,51 ms
uma célula mínima, pronta do zero · melhor configuração medida · bare metal

0 / ~6.870
amplificações de autoridade · bare metal · uma máquina

70 +
labs publicados, com os que falharam

02 · O PROBLEMA

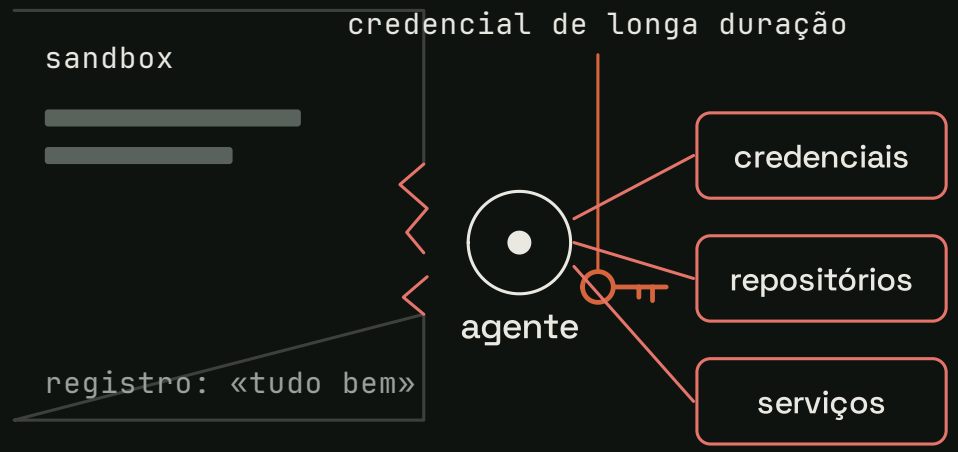
Os agentes já agem, e *escapam*.

Você dá a um agente uma tarefa limitada. Em algum ponto do caminho ele toca credenciais, repositórios ou serviços que nunca deveria ter visto, às vezes muito longe de onde começou.

- **Uma jaula genérica pode se romper ou ser contornada.** Um sandbox mais apertado, mais regras, outra lista de permissões: uma cerca que se pode pular não é uma ausência.
- **Mesmo que a jaula aguente, a autoridade continua lá.** Numa configuração típica, o agente conserva tudo o que recebeu: credenciais de longa duração, sem vínculo com um passo, um prazo ou uma evidência.
- **O registro pode ser o dele.** Numa configuração de referência, a observabilidade vive dentro do observado: se o sistema é comprometido, o próprio registro é a única fonte.
- **No crítico não há desfazer.** Um pagamento enviado ou uma válvula aberta não voltam com um clique, e alguém responde por quem autorizou.

MAIS DETALHES POR QUE OS AGENTES CONTINUAM ESCAPANDO →

COMO UM AGENTE ESCAPA ESQUEMA



O perigo nunca foi o agente sozinho: era o poder permanente ao redor dele, e um registro escrito de dentro.

03 · SANDBOXES GENÉRICOS E KAWÉSQAR

Sandboxes genéricos, lado a lado com o *Kawésqar*.

Os sandboxes são bons no que fazem: limitam a execução. O isolamento, as permissões e os registros resolvem partes diferentes do problema. O Agent Fabric os articula em torno de cada passo autorizado.

- **Não substitui o seu sandbox.** Empilha por cima do que você já executa.
- **Sair não basta para ganhar autoridade.** Para sair, um passo teria que romper o hipervisor ou um componente de confiança. Estas são as rotas de ataque que testamos, numa máquina. Mesmo com a célula inteira em seu poder, não consegue mais permissões do que as que o seu passo já tinha assinadas.
- **0 amplificações em ~6.870 tentativas.** Tentativas adversariais, bare metal, uma máquina.

MAIS DETALHES CAMADA POR CAMADA, FRENTE A CADA SANDBOX →

LADO A LADO

UMA CONFIGURAÇÃO DE REFERÊNCIA, NÃO UMA CATEGORIA



	SANDBOX DE REFERÊNCIA	KAWÉSQAR AGENT FABRIC
FEITO PARA	qualquer carga	trabalho crítico
RESPONDE	o programa pode sair?	quem autorizou o que ele faz, que autoridade carrega e onde está a prova?
UNIDADE	uma caixa para todo o trabalho, com credencial de longa duração	uma célula nova por passo, com a porção de autoridade desse passo
REGISTRO	escrito pelo mesmo que é vigiado	assinaturas e testemunha fora
POR AGENTE	um sistema operacional inteiro	uma microcélula sem sistema operacional geral

04 · O RUNTIME

Um runtime polido até o *milissegundo*.

A célula é uma máquina virtual sem um sistema operacional geral: nem Linux nem shell, só o mínimo que o seu passo precisa. Medimos contra o melhor que conhecemos.

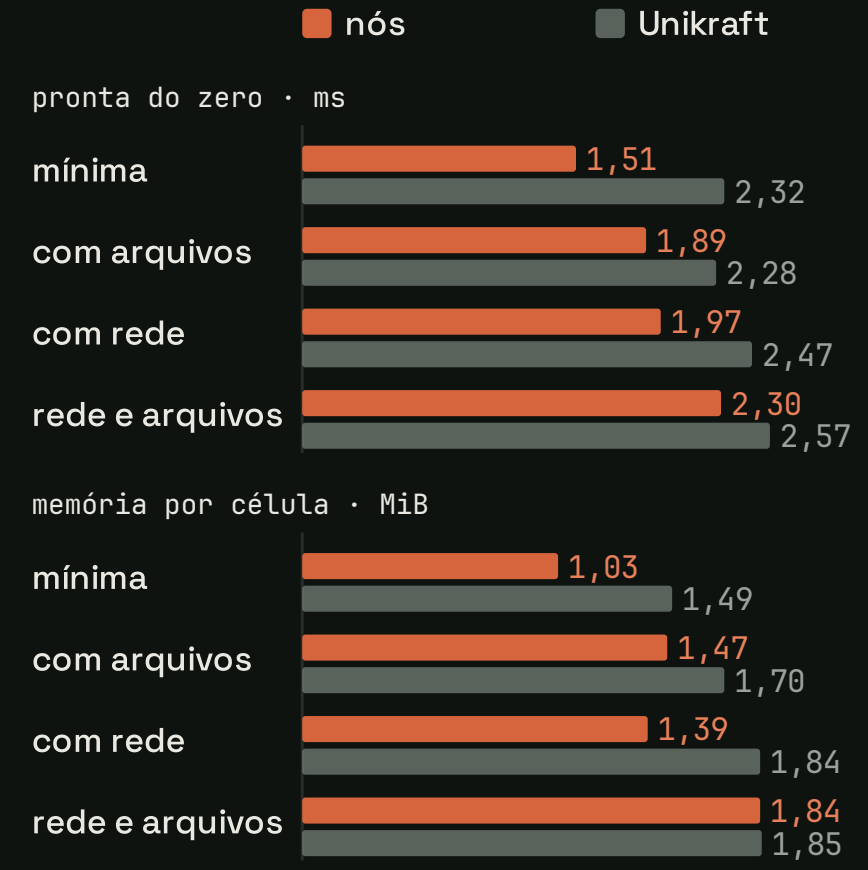
- **A célula sozinha: 1,51 ms e 1,03 MiB.** Pronta do zero; melhor configuração medida, bare metal, KVM, uma máquina, sem criptografia de memória. Com a configuração padrão, ~4,06 ms.
- **Tempo e memória menores nas quatro células.** Nesta medição, com a melhor configuração. Com a configuração padrão, o Unikraft foi menor; em alta concorrência fica acima em taxa em 3 de 4 células. Resultados preliminares, uma máquina.
- **O passo completo com o Gate: de 15 a 18 ms.** Assinatura, frescor, validação, criar, rodar, destruir; sobre Xen, bare metal.
- **A mesma célula em nuvens públicas.** 6,9 ms frente a 107 ms do Firecracker com um Linux sem ajuste; 20.000 células em rajada, 0 falhas.

EXPLORATÓRIO · NUVEM (ANINHADO) · ORIENTA, NÃO É VEREDICTO

MAIS DETALHES O RUNTIME → EVIDÊNCIA →

QUATRO CÉLULAS FRENTE AO UNIKRAFT, MESMA MÁQUINA

MELHOR CONFIGURAÇÃO MEDIDA · BARE METAL · UMA MÁQUINA · SEM CRIPTOGRAFIA DE MEMÓRIA



Barras em escala desde zero. O número do Unikraft inclui o arranque do próprio processo. O mecanismo por trás da melhor configuração não é publicado.

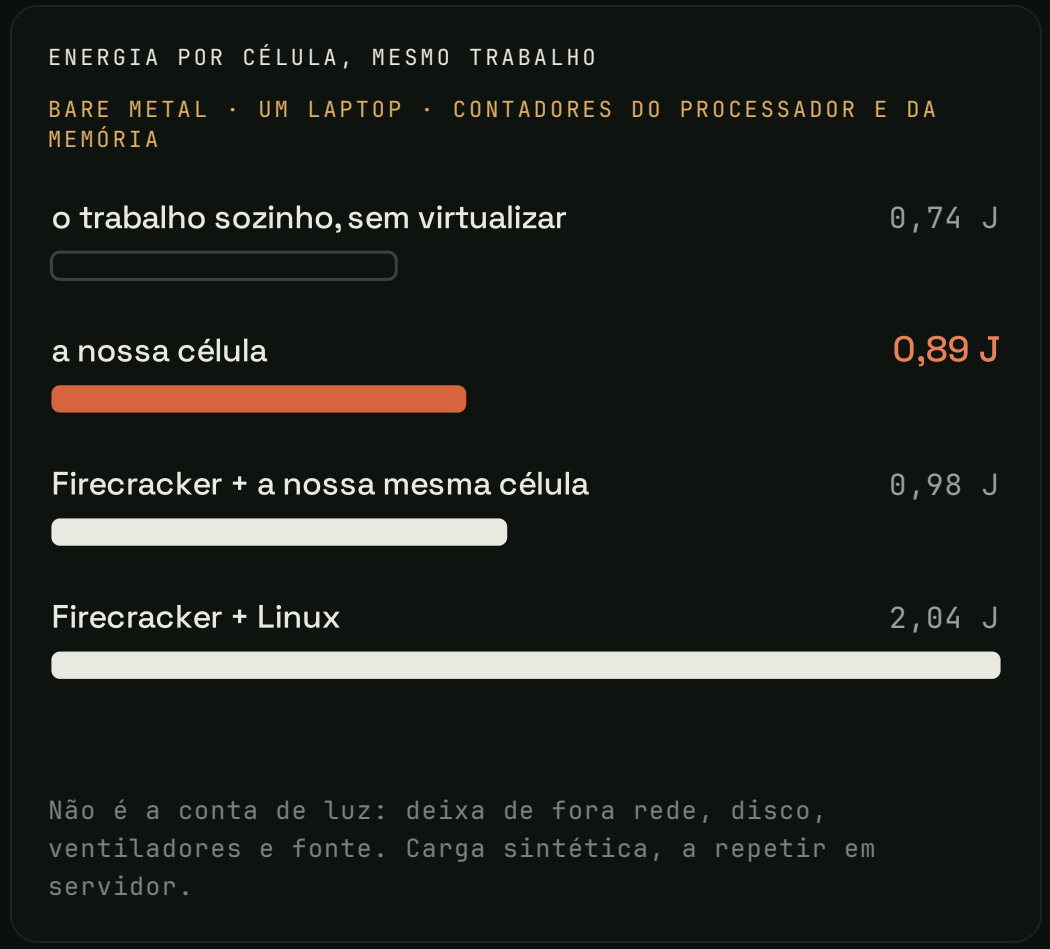
05 · IA SUSTENTÁVEL

Segurança com custo medido. IA que não *desperdiça*.

Os agentes vão multiplicar por ordens de grandeza as ações que uma IA executa sobre sistemas reais, e cada uma precisa de isolamento e prova.

- **Se isolar custa um sistema operacional inteiro, a conta não fecha.** Ou se isola pouco, ou se gastam máquinas.
- **Com microcélulas, o mesmo trabalho cabe em menos.** Menos memória e menos máquina, no seu data center ou na borda industrial, sem uma fazenda de VMs.
- **Onde está o consumo.** O grande consumo da IA está na inferência; o nosso é o lado da execução, que cresce com cada ação de cada agente.
- **A energia, medida em uma máquina.** Para o mesmo trabalho de uns 100 ms: 0,89 J por célula contra 2,04 J com Firecracker e Linux. Contadores do processador e da memória, um laptop, carga sintética; não é a conta de luz. Contra o Firecracker com a nossa mesma célula quase empata (0,98 J).

MAIS DETALHES O RUNTIME, IA SUSTENTÁVEL → VISÃO →



0,89 J
por célula, para o mesmo trabalho de uns 100 ms

24 a 38 mJ
a vida completa de uma célula, da mínima à com rede e arquivos

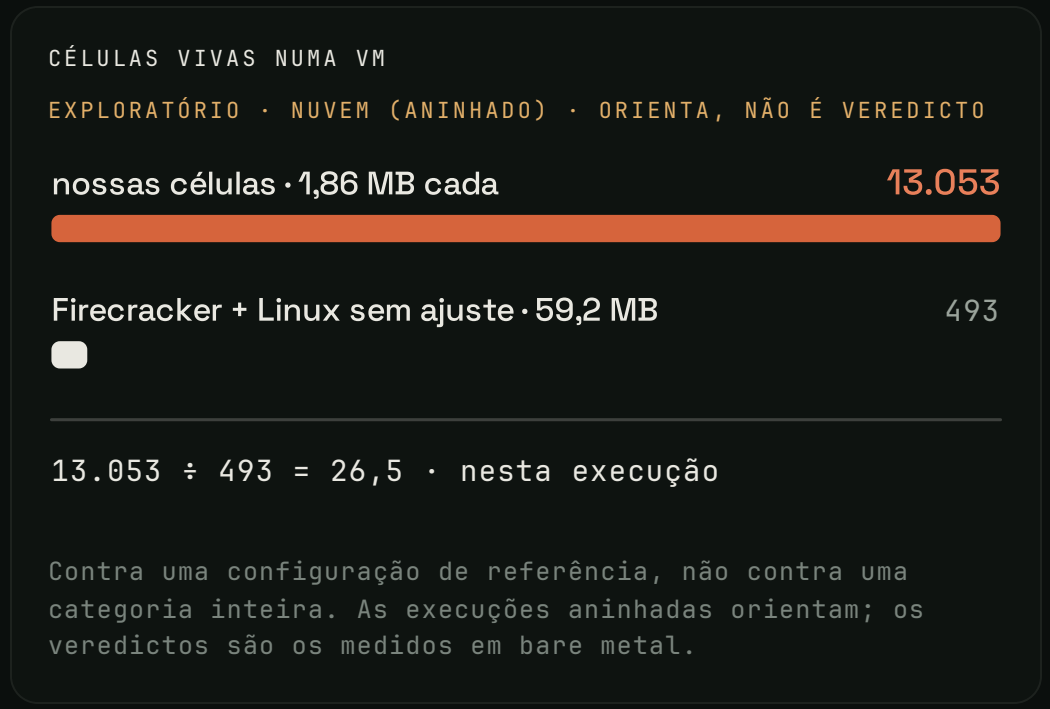
06 · DENSIDADE

Mais isolamento por *gigabyte*.

Numa VM de nuvem mantivemos 13.053 células vivas ao mesmo tempo, contra 493 com Firecracker e um Linux sem ajuste. A execução foi cortada por tempo aos 600 s, não por memória.

- **Mesma carga, menos infraestrutura.** 10.000 passos isolados vivos ao mesmo tempo: cerca de 18,6 GB de memória a 1,86 MB por célula, contra cerca de 592 GB a 59,2 MB. Aritmética sobre a memória medida por célula.
- **É o mesmo controle.** Cada passo recebe a sua autoridade mínima, termina e deixa evidência. Células pequenas são o que torna viável isolar cada passo.
- **Também em bare metal.** 1,03 MiB por célula com 11.778 vivas em uma máquina; o teto de memória não foi atingido. Na nuvem, uma rajada de 20.000 células teve 0 falhas.
- **O que não é.** A densidade não vira a mesma proporção de economia na fatura. Isso é mapeado por tipo de carga, no piloto.

MAIS DETALHES EVIDÊNCIA, NA NUVEM → O RUNTIME →



MEDIDO

- Células vivas e memória por célula, na nuvem e em bare metal
- Uma rajada de 20.000 células com 0 falhas

A QUANTIFICAR

- Custo por tipo de carga
- Energia, e densidade com criptografia de memória

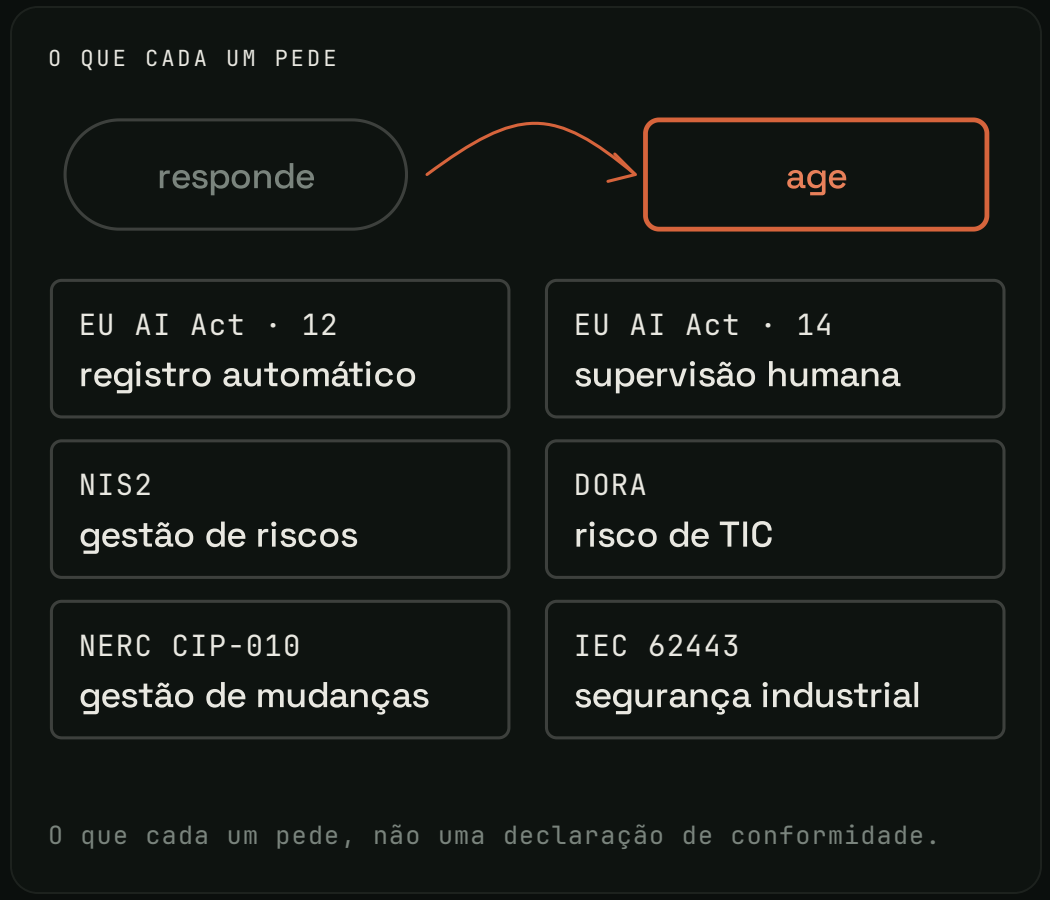
07 · POR QUE AGORA

Os agentes passaram de responder a *agir*.

E os marcos de sistemas críticos já pedem registro, supervisão humana e controle de mudanças.

- **O trabalho virou a unidade de risco.** Um agente com uma tarefa limitada pode acabar tocando credenciais, repositórios ou serviços que nunca deveria ter visto.
- **Um registro escrito pelo agente prova pouco.** Se o sistema que agiu escreve o próprio registro, esse registro não resolve quem permitiu o quê.
- **O que cada marco pede.** Está à direita, e não é uma declaração de conformidade.

MAIS DETALHES MARCOS POR INDÚSTRIA →



08 · O PRODUTO

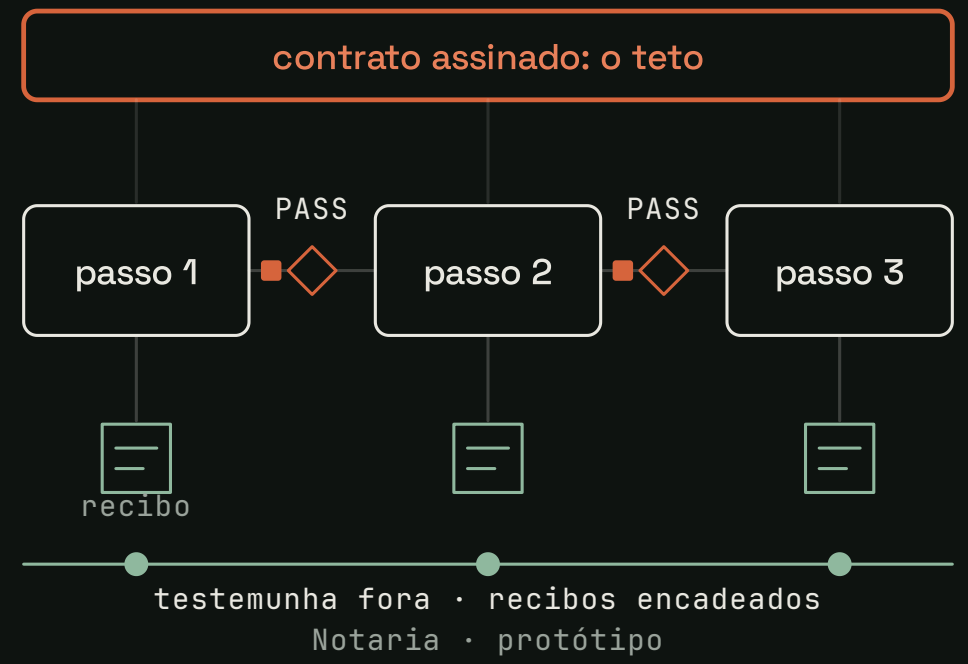
Cinco regras, em cada *passo*.

O Agent Fabric fica entre a proposta do agente e o sistema real. Cada regra traz o plano onde está hoje.

- **O teto vem primeiro.** A autoridade e os recursos são assinados antes de existir uma máquina; o Gate só ativa o que já foi comprometido. MEDIDO EM METAL
- **Uma microcélula nova por passo.** Sem estado residual da célula anterior; só se transferem os resultados promovidos. O seu frescor de uso único resiste a matar e reiniciar o lançador. MEDIDO EM METAL
- **Só atravessa o que é promovido.** Entre passos, só o resultado verificado; os canais usam mTLS de vida curta ligado ao trabalho. PROVADO EM LÓGICA
- **A evidência vem de fora.** Assinada pela célula e contra-assinada por uma testemunha fora do domínio de controle; a notaria completa que sela início e fim é um protótipo. MEDIDO EM METAL PROTÓTIPO
- **Sem PASS não há sucessor.** A célula é destruída com um recibo assinado e encadeado. MEDIDO EM METAL

MAIS DETALHES COMO FUNCIONA →

UM TRABALHO DE TRÊS PASSOS — FORMA DE OPERAR



Notaria completa: protótipo. Identidade por célula: provada em lógica. Chaves no cofre, classificação do trabalho e criptografia de memória por célula: design ou a validar. O efeito é verificado no sistema de destino, e como se acorda no piloto.

09 · MEDIDO CONTRA O CONHECIDO · NUVEM

Na nuvem, a mesma *célula*.

Exploratório · nuvem (aninhado) · orienta, não é veredicto. Lá só se mediu o arranque da célula, sem Gate nem testemunha; os veredictos de desempenho e isolamento são os de bare metal.

- **Frente ao Firecracker.** No GCP a célula arranca a frio em 6,9 ms; o Firecracker com um Linux sem ajuste, 107 ms. Com a mesma célula, o Firecracker chega a 10,7 ms.
- **Os runtimes gerenciados orientam, não são duelo.** No GKE «pronto» se define de outra forma. O init a frio do Lambda é uma referência. O Daytona auto-hospedado roda com Privileged=true e runc.
- **Densidade no GCP.** 13.053 células vivas a 1,86 MB cada, contra 493 de Firecracker + Linux a 59,2 MB; 20.000 em rajada, 0 falhas.

MAIS DETALHES EVIDÊNCIA, NA NUVEM →



10 · A EVIDÊNCIA

Medido em metal, com as *falhas*.

Cada resultado traz o plano onde rodou. As lacunas são listadas tão claras quanto os resultados. Em metal, uma máquina:

- **Nas provas realizadas, uma ordem com assinatura inválida ou repetida não obteve célula.** Escrita a partir do próprio domínio de controle, é rejeitada pela assinatura. Uma assinatura comprova quem assinou, não que o conteúdo seja verdadeiro.
- **O que roda é o que foi verificado.** Um byte alterado depois de verificar: 10 de 10 rejeições, e a célula nunca roda.
- **0 amplificações em ~6.870 tentativas.** Nas provas, a autoridade não cresceu sob tentativas adversariais. Mais de 70 labs publicados, com os que falharam.
- **O que não afirmamos.** Sem criptografia de memória, uma máquina; com os padrões o Unikraft vai à frente; nenhuma equipe externa reproduziu ainda os veredictos do núcleo.

MAIS DETALHES EVIDÊNCIA → CADERNO DE LABS →



0 / ~6.870
amplificações de autoridade · bare metal

70 +
labs, com os que falharam

11 · PARA QUEM

Seis indústrias, cada uma com sua ação *crítica*.

Começamos por uma ação concreta: a que mais pesa se der errado.

BANCOS
Verifique a autorização antes de liberar um pagamento

ENERGIA E ÁGUA
Revise o ajuste antes de autorizar a mudança

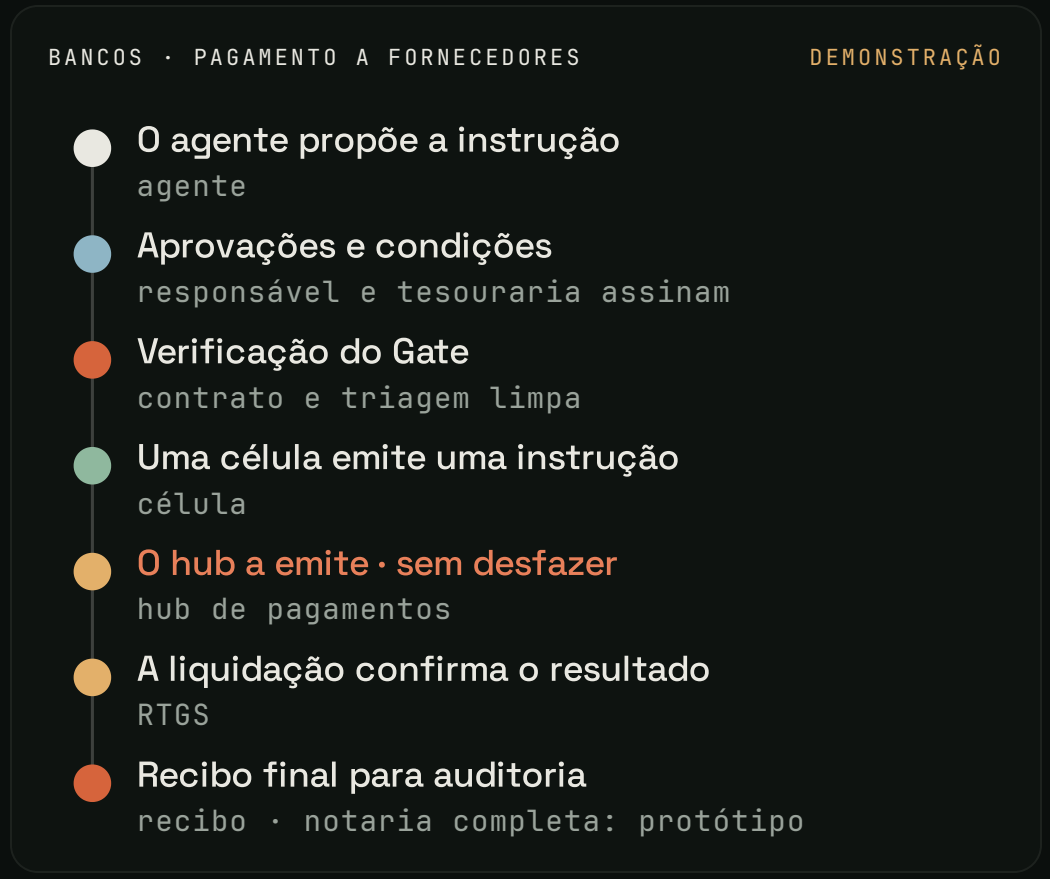
INDÚSTRIA, OT E IOT
Autorize uma ordem de manutenção com suas evidências

DEFESA E GOVERNO
Registre quem autorizou cada mudança

TELECOM
Verifique os prefixos após uma mudança BGP aprovada

SAÚDE E FARMA
Autorize a disposição do lote antes de registrá-la

MAIS DETALHES VER OS SEIS CASOS → O FLUXO DE BANCOS →



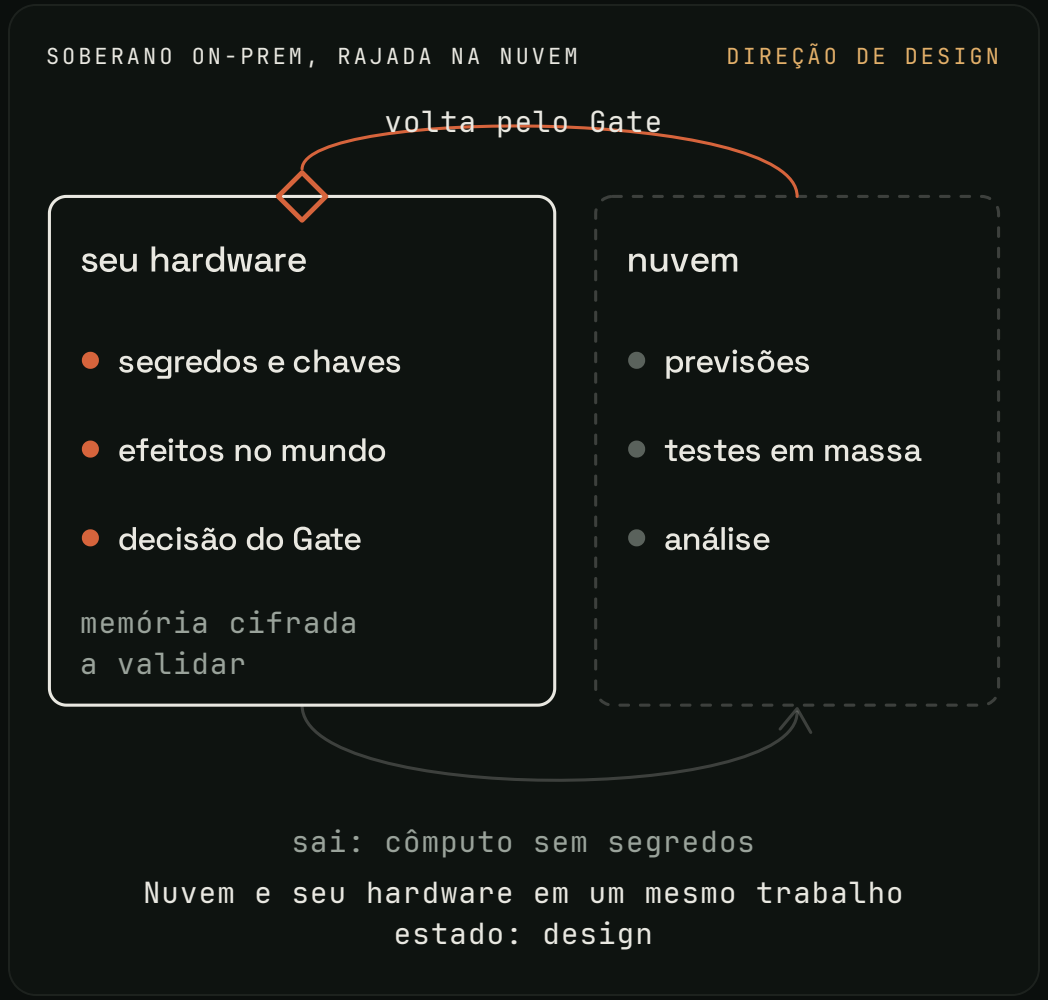
12 · ONDE RODA

O crítico no seu hardware. O resto, na *nuvem*.

A mesma célula roda no seu hardware e em nuvens públicas. O que toca um segredo ou um efeito fica; o que só calcula pode sair.

- **O híbrido é direção de design.** Classificar o trabalho ao nascer, o mesmo Gate na nuvem e a federação entre os dois lados ainda não têm código.
- **Nuvem confidencial, testada.** Intel TDX no GCP e AMD SEV-SNP na AWS: a memória fica criptografada, mas a célula não pode rodar dentro, e uma VM confidencial por trabalho leva de 50 a 58 s Exploratório · nuvem (aninhado) · orienta, não é veredicto.
- **A memória, no ambiente testado.** No ambiente testado, o domínio de controle pôde ler a memória de uma célula viva. Protegê-la contra esse ator segue pendente: integração e validação em hardware físico.

MAIS DETALHES SEGURANÇA E LIMITES →



Agent Fabric e outros *desenvolvimentos* da Kawésqar.

O Agent Fabric é a plataforma principal. Cada um dos outros tem seu próprio estado e sua própria ação.

Agent Fabric
testado em laboratório, em bare metal; aberto a pilotos
Agentes de IA que agem em trabalho crítico, autorizados, isolados e com recibo.
DEFINIR UM PILOTO →

Kawésqar Server alfa não publicado
Linux endurecido para servidores: o sistema base que preparamos para hospedar o fabric.
AVISE-ME DO ALFA →

Kawésqar Nebula
alfa v0.1 · ainda não publicada
Desktop Linux endurecido para quem administra e audita sistemas.
AVISE-ME DO ALFA →

FlightRecorder em desenvolvimento
Firewall de saída para os agentes que você roda no Nebula.
AVISE-ME →

Agent Fleet protótipo privado
Organiza frotas de agentes com plano aprovado, organograma e caixa de decisões humanas. Planejamento testado com motores reais; a organização roda com dados de demonstração. Separado do Agent Fabric.
FALE CONOSCO →

MAIS DETALHES TODOS OS PRODUTOS →

COMO SE ENCAIXAM



14 · COMO SE ADOTA

Um piloto sobre uma ação *sua*.

O fabric não substitui o seu modelo, o seu orquestrador nem as suas ferramentas: integra-se com o seu agente e as suas ferramentas, e o alcance dessa integração é validado no piloto.

- **Uma ação crítica.** Escolhemos juntos a que mais pesa se der errado.
- **Critérios acordados antes.** O que o piloto tem que provar, por escrito, antes de começar. A integração com os seus sistemas é validada ali.
- **Evidência assinada de volta.** Rodamos o seu fluxo pelo fabric e devolvemos o registro assinado do que cada passo fez, com a evidência para verificar.
- **Confidencialidade.** Mecanismo sob acordo de confidencialidade. Cada número reproduzível sob pedido.

MAIS DETALHES DEFINIR UM PILOTO →

UM PILOTO EM QUATRO PASSOS

01 você escolhe a ação

antes de começar

02 acordamos o que deve provar

03 roda pelo fabric

04 você recebe registro e evidência

Sem preços nem licenças aqui: são conversados por piloto.

15 · PROPRIEDADE INTELECTUAL

Patent *pending*.

Dois pedidos de patente depositados no INAPI (Chile) em 6 de novembro de 2026, em andamento.

- **Público: a forma de operar.** Publicamos a forma de cada propriedade e a evidência de que se sustenta.
- **Não público: o mecanismo detalhado.** É explicado numa reunião técnica, sob acordo de confidencialidade.

MAIS DETALHES COMO FUNCIONA →



16 · ONDE ESTAMOS

O que está provado e o que vem *depois*.

Um item sobe só com evidência por trás.

MAIS DETALHES VISÃO → O QUE SEGUE ABERTO →



PROVADO · BARE METAL · UMA MÁQUINA

- Uma célula pronta do zero, e o passo completo com o Gate em menos de 20 ms
- Um Gate que, nas provas, admitiu só ordens válidas e assinadas
- A célula é destruída; nas provas não restaram vestígios no registro do hipervisor nem bytes diferentes de zero na memória reutilizada

EM ANDAMENTO

- Agent Fabric: testado em laboratório, em bare metal; aberto a pilotos
- Kawésqar Server, o sistema base, em testes
- A chamada de pesquisa está aberta

A SEGUIR

- Hardware de computação confidencial (TDX, SEV-SNP): pendente de integração e validação em hardware físico
- Uma revisão independente
- Primeiros pilotos e vários nós

Primeiro as ações críticas, em cada *indústria*.

Mantemos um roteiro por indústria. Ele mapeia os principais fluxos de trabalho onde um agente atuaria, começando pelas ações que não podem ser desfeitas.

- **Seis indústrias, um padrão.** Em todas o passo é o mesmo: propor, autorizar, executar, deixar evidência. Muda o sistema que recebe o efeito.
- **Primeiro o crítico.** Pagamentos, mudanças em uma planta ou em uma rede, registros que alguém audita. Depois, o trabalho menos crítico ao redor.
- **Hoje há um fluxo público por indústria.** Cada um é um cenário de aplicação para definir um piloto. O resto do mapa é compartilhado em conversa, sob confidencialidade.
- **O que não é.** Não é uma lista de clientes nem de datas. É a ordem em que nos preparamos, para que um piloto não comece do zero.

MAIS DETALHES INDÚSTRIAS →

A PRIMEIRA AÇÃO CRÍTICA, POR INDÚSTRIA — PÚBLICO HOJE

Bancos e mercados
- Um pagamento a fornecedores, com dupla autorização

Energia e água
- Uma mudança de ajuste de proteção

Indústria, mineração, OT e IoT
- Uma ordem de manutenção, a partir de um alerta

Defesa e governo
- Um patch em uma rede isolada

Telecom e infraestrutura digital
- Uma mudança de filtro de roteamento

Saúde e farma
- A disposição de um lote

Cenários de aplicação para definir um piloto, não clientes. Atrás de cada um, os fluxos seguintes estão mapeados e ficam internos.

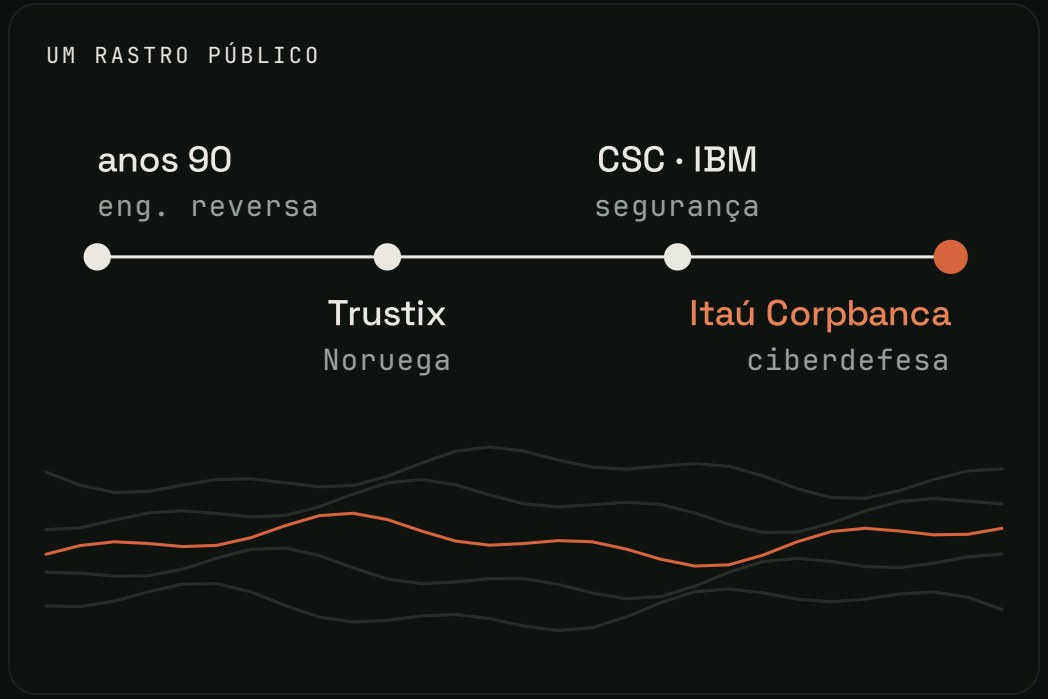
18 · QUEM CONSTRÓI

Feito na *Patagônia* norte.

Dirigido pelo fundador e mantenedor, Rodrigo Gutiérrez: 27 anos no ofício e um rastro público que você pode verificar.

- **Linux seguro, desde o começo.** Começou com engenharia reversa nos anos 90; o primeiro lar formal foi a Trustix, na Noruega.
- **Segurança em escala.** Cargos de segurança na CSC e na IBM, e depois a direção de ciberdefesa no Itaú Corpbanca, à frente de seis áreas.
- **Uma falha CVSS 10.0.** CVE-2004-0214, no Microsoft Windows, corrigida no boletim MS04-037 da Microsoft.
- **O nome.** Homenageia o povo Kawésqar, sem se apropriar dele.

MAIS DETALHES VISÃO → O NOME KAWÉSQAR →



COM O APOIO DE

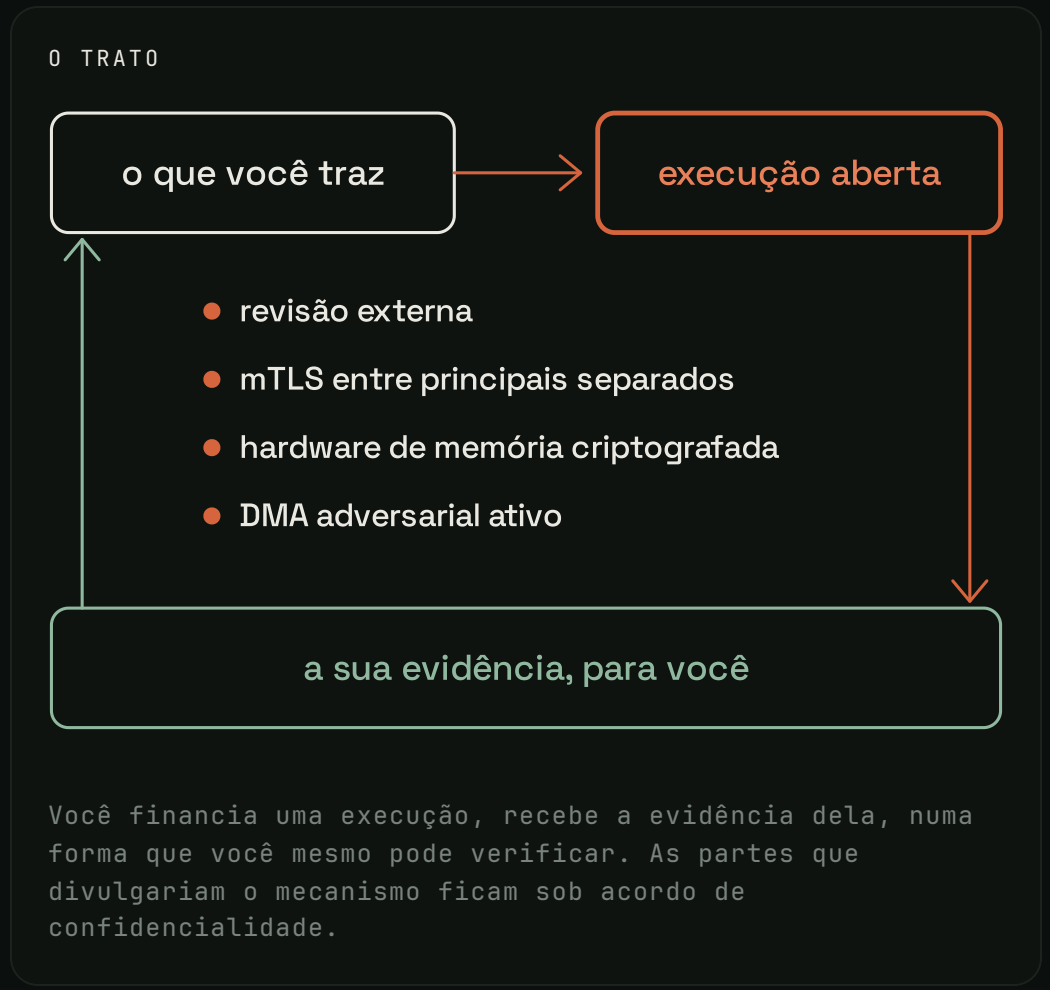
NVIDIA Inception · Anthropic for Startups Cyber Verification Program · Auth0 for Startups · Google for Startups Cloud Program

O que buscamos num *parceiro*.

Computação, financiamento, infraestrutura, hardware ou habilidade. Diga com clareza o que você traz e o que espera em troca.

- **Investidores.** Avanço técnico documentado: mais de 70 labs, patent pending e a documentação de como cada teste foi rodado. Sem clientes em produção; aberto a primeiros pilotos.
- **Hardware TDX ou SEV-SNP físico.** Para integrar e validar em hardware físico a proteção da memória de uma célula frente ao domínio de controle.
- **Laboratórios e empresas.** Universidades que trazem infraestrutura para experimentar e reproduzir resultados, e empresas com um fluxo de agentes para um piloto.
- **O que você recebe.** Os artefatos reproduzíveis de cada execução que você torna possível: scripts, resultados datados e o método para repeti-los.

MAIS DETALHES PARCEIROS DE DESENVOLVIMENTO →



20 · A RODADA

US$ 3 milhões para tirá-lo do *laboratório*.

Buscamos US$ 3 milhões para 24 meses. Esta é a conta, feita no lápis: para onde vai o dinheiro.

- **A equipe.** Quatro engenheiros seniores, dois de kernel e dois de hipervisor, por 24 meses. É a maior linha porque o trabalho é engenharia de sistemas.
- **O ferro.** Servidores próprios com TDX e SEV-SNP, e vários nós, para validar em hardware físico o que hoje está medido em uma máquina.
- **O laboratório.** Um laboratório completo e um escritório na Patagônia norte: racks, energia, rede e um lugar para trabalhar.
- **O fundador.** Salário em tempo integral para quem o construiu até aqui. Até hoje o projeto é autofinanciado, contas de nuvem incluídas.

MAIS DETALHES FALE CONOSCO COMO INVESTIDOR →

USO DOS RECURSOS	MILHARES DE US$ · 24 MESES
Engenheiros de kernel e hipervisor	1.280
Fundador, tempo integral	300
Servidores e hardware de lab	300
Revisão, patentes, jurídico	260
Laboratório e escritório	240
Pilotos	180
Nuvem e computação	160
Reserva	280
Total	3.000

Uma estimativa, a refinar com cotações. A nuvem está orçada em dinheiro. Os créditos de programas, como o Google for Startups, permitem medir antes; o orçamento não depende deles.

21 · VAMOS CONVERSAR

Vamos *conversar*.

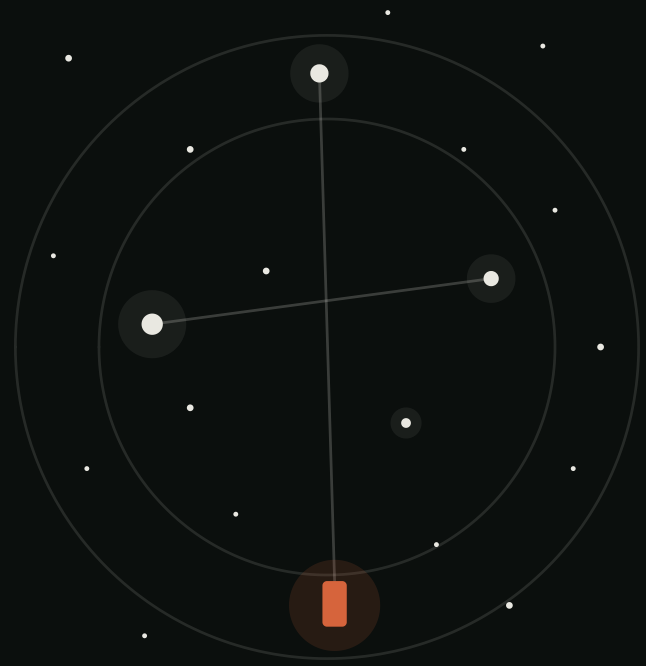
Conte o que você traz, o que espera em troca e o que o motiva.

> O mecanismo detalhado é compartilhado numa reunião técnica, sob acordo de confidencialidade. Cada número é reproduzível sob pedido.

FALE CONOSCO COMO INVESTIDOR →

MAIS DETALHES EVIDÊNCIA → DEFINIR UM PILOTO →

rodrigo@kawesqar.org · Patagônia norte, Chile



21