ARQUITECTURA ZERO TRUST AVANZADA

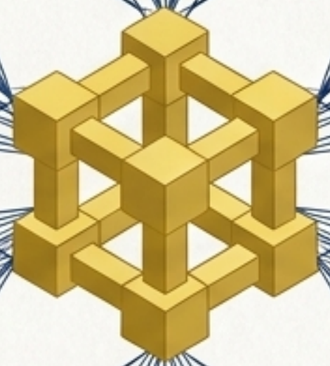
MODELO DE CONFIANZA CRIPTOGRÁFICA DISTRIBUIDA

SkyDefended InfraApp v1.2: Establecimiento, validación autónoma y continuidad de confianza en runtimes efímeros.

NEXOCYBER NETWORKS

NCN

NETWORKING, SEGURIDAD Y SISTEMAS

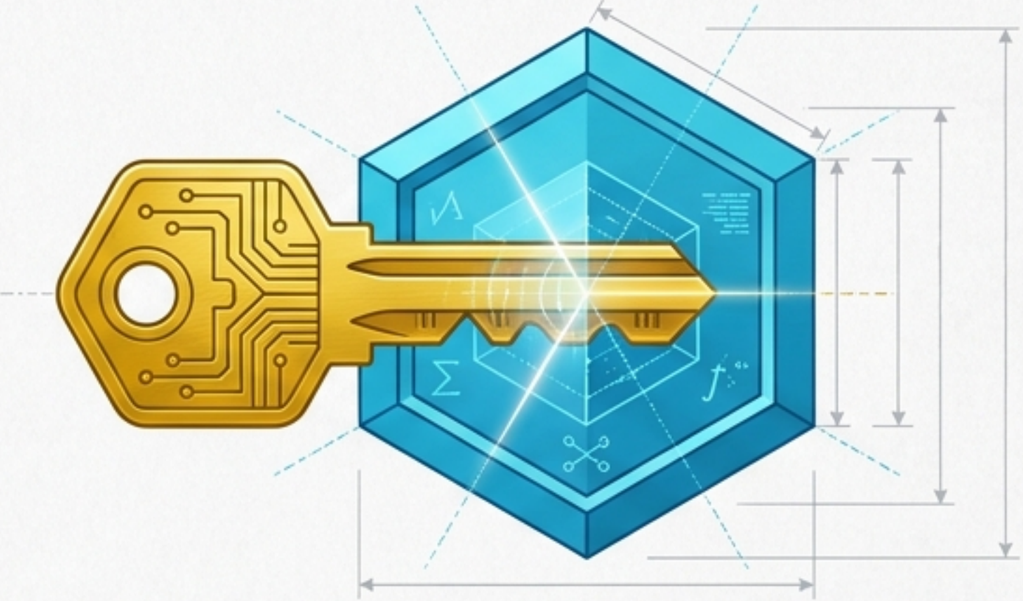


La confianza estructural no se infiere; se demuestra matemáticamente

El Dónde y El Cómo

Transporte Topológico (Efímero)

El Con Quién



Identidad Matemática (Inmutable)

Explícita y Previa
Establecida antes del primer byte funcional.

Criptográfica
Basada en identidades persistentes, no topología.

Mediada
Definida exclusivamente por el Plano de Control.

Local
Validada matemáticamente en el nodo receptor.

Desacoplando el transporte efímero de la autoridad inmutable

Transporte y Exposición

NO constituyen confianza

- Direcciones IP y Redes Privadas
- Proxies y Frontends Web
- Entornos de Ejecución e Instancias Físicas
- Sesiones HTTP

Participan en conectividad operacional, jamás en autoridad criptográfica.

Autoridad Criptográfica

SÍ constituyen confianza

- Claves RSA Aisladas (2048+ bits)
- Distribución JWKS y Firmas RS256
- Identificadores Criptográficos (kid)
- Tokens JWT de Identidad Operacional

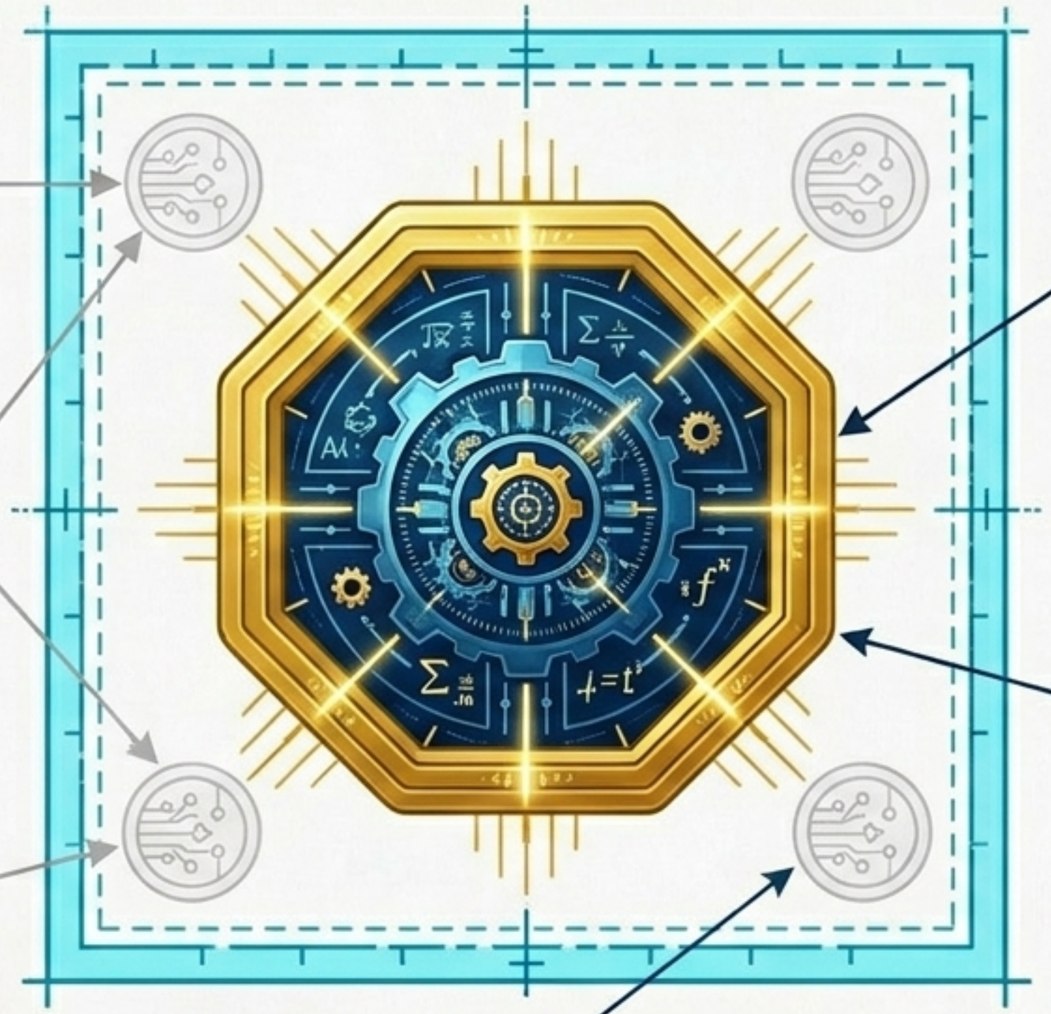
Elementos inmutables, auditables y matemáticamente verificables.

Las cápsulas escalan la operación; los Engines custodian la confianza

Frontends
(Periferia Operacional)

Relación estructural intrínseca por despliegue. NO firman, NO validan, NO mantienen autoridad criptográfica.

Persistencia Funcional



Única entidad con **identidad criptográfica (Clave Privada, Pública, kid)**.

Las claves privadas NUNCA abandonan este perímetro.

El Engine
(Núcleo Autoritativo)

Estricta separación de datos de negocio respecto a la persistencia criptográfica.

Singularidad arquitectónica frente a escalabilidad operacional

Nivel 1: Plano de Control (El Árbitro Criptográfico)

Singularidad: Única cápsula principal (Root of Trust).

Función: Define identidades, construye relaciones, distribuye artefactos firmados. Jamás consume operaciones de negocio.

Nivel 2: Plano de Acceso (Identidad Operacional)

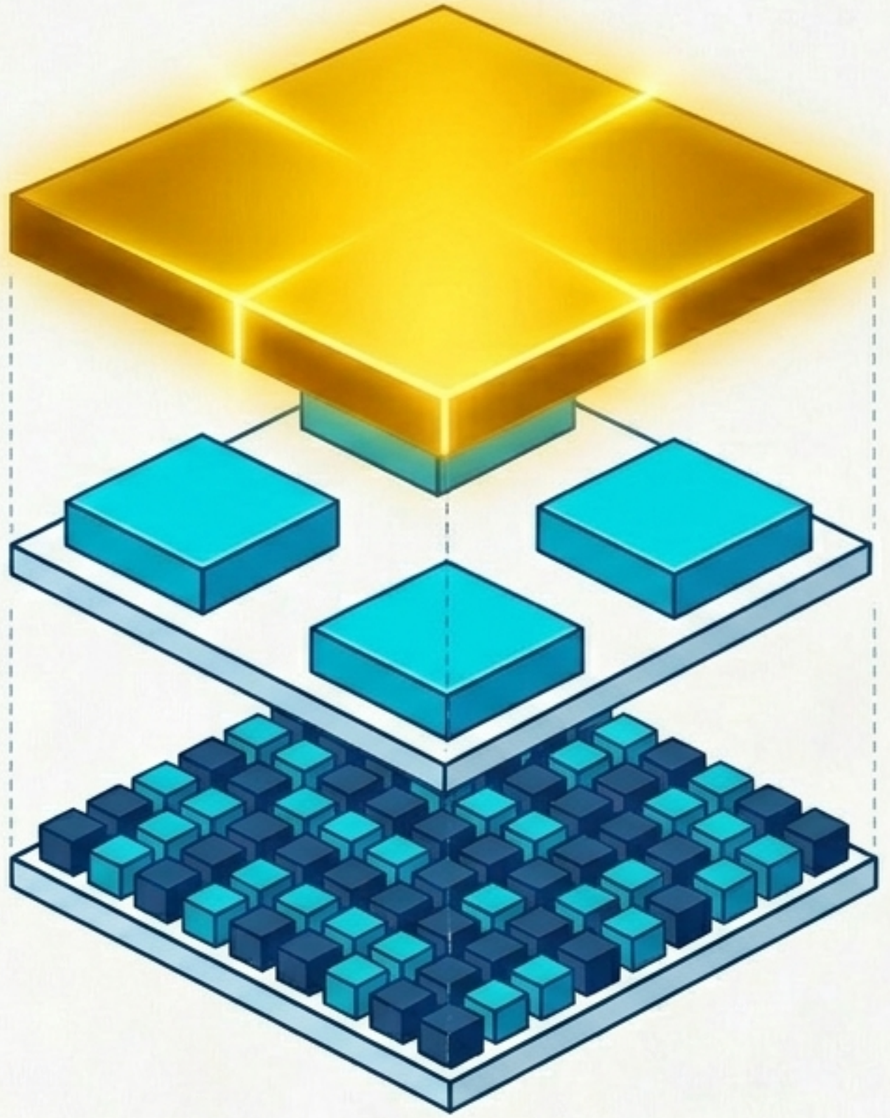
Escalabilidad: Engines distribuidos por región o tenant.

Función: Genera identidades operacionales en base a las políticas del Control.

Nivel 3: Plano de Aplicación (Lógica de Negocio)

Escalabilidad: Miles de cápsulas funcionales.

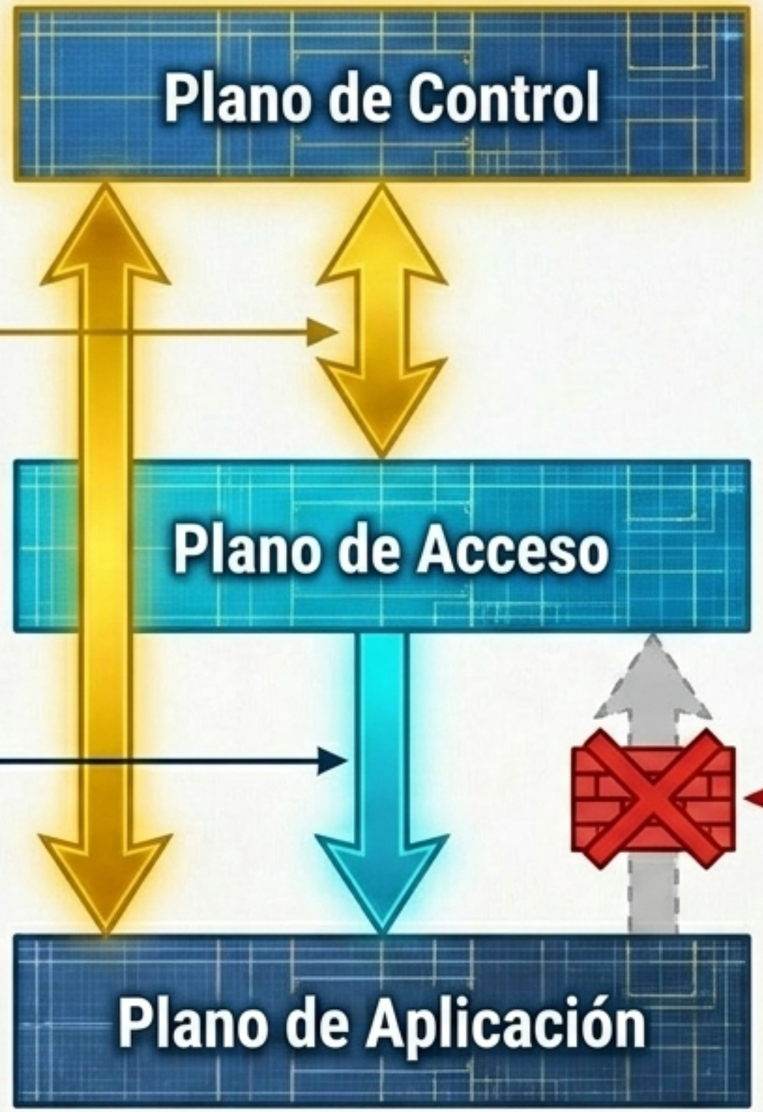
Función: Valida firmas de entrada y ejecuta procesos de negocio aislados.



Distribución asimétrica basada en privilegio mínimo criptográfico

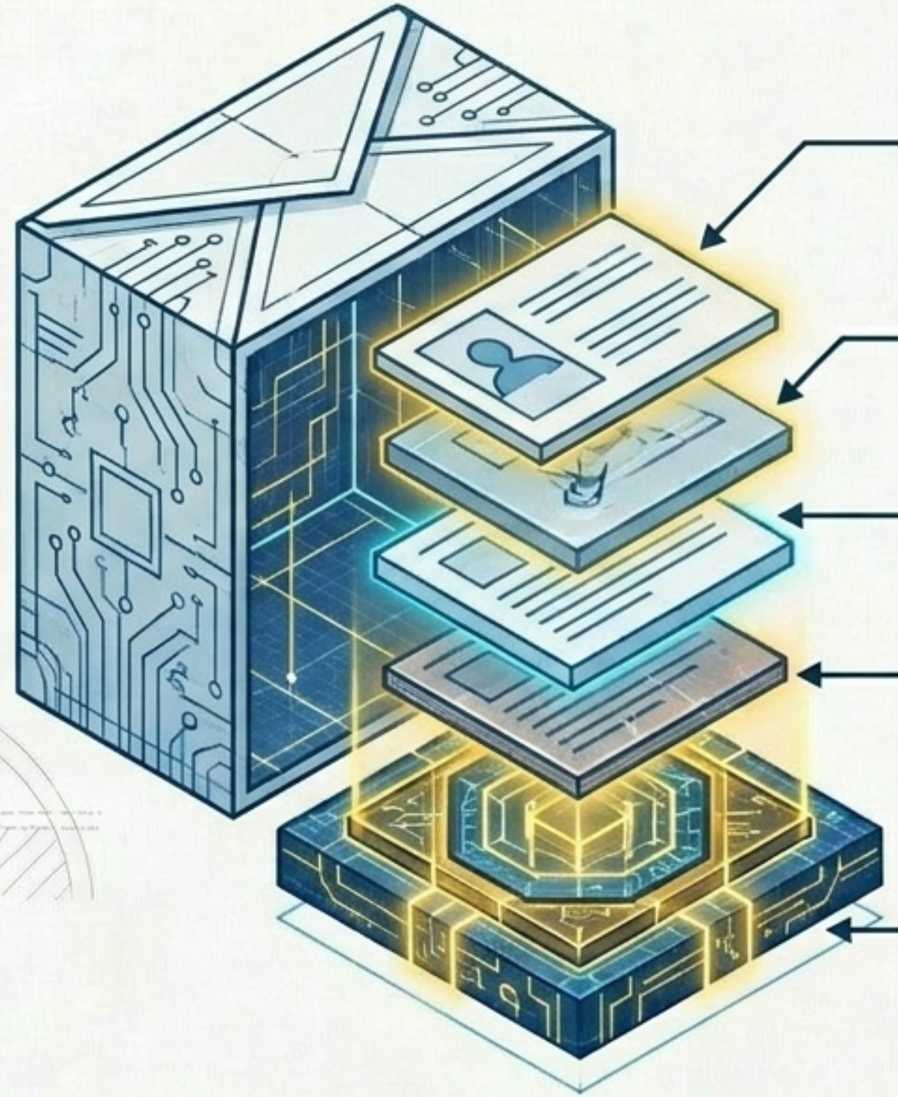
Distribución Bidireccional:
Control distribuye claves y metadatos. Engines registran identidad y demuestran pertenencia.

Emisión de Identidad:
El Acceso emite identidad operacional (JWT). La Aplicación valida y consume.



Regla de Oro:
La aplicación NO emite identidad hacia el acceso. Confianza mínima estricta.

Mecánica de distribución: Empaquetando el contexto criptográfico



Identidades autorizadas

JWKS
(Claves públicas)

Restricciones contextuales

Artefactos de revocación explícita

Firma Digital
RS256

Flujo de Aceptación

1. Recepción

Engine recibe Policy Bundle.

2. Validación de Origen

Receptor verifica firma RS256 usando la clave pública conocida del Control Plane. Ningún bundle no firmado es procesado.

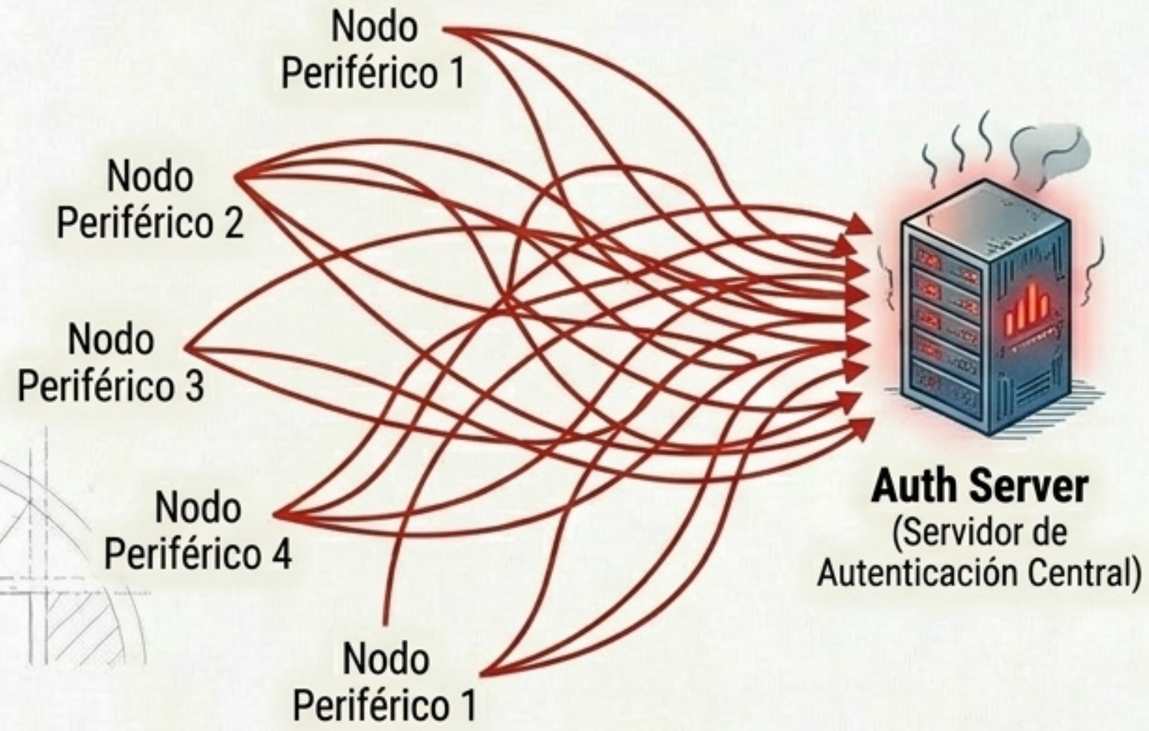
3. Aplicación Local

Se aplican las políticas distribuidas. No existe confianza horizontal implícita.

Validación in-memory autónoma: Desacoplando el runtime del Control

Modelo Centralizado

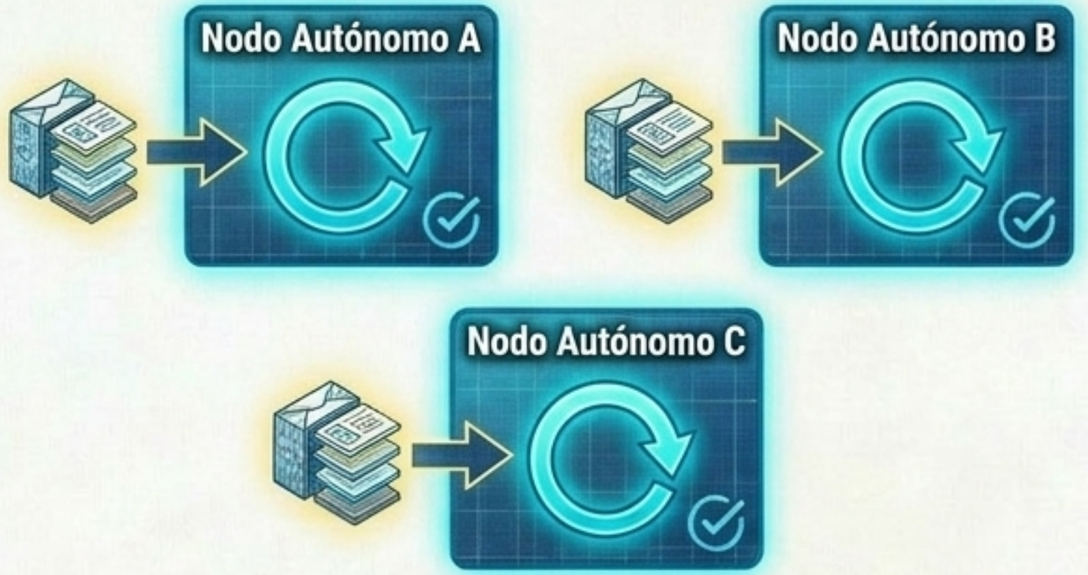
Latencia + Fragilidad



- Cada interacción requiere consulta síncrona.
- Si el Plano de Control cae, la plataforma se paraliza.

Modelo SkyDefended

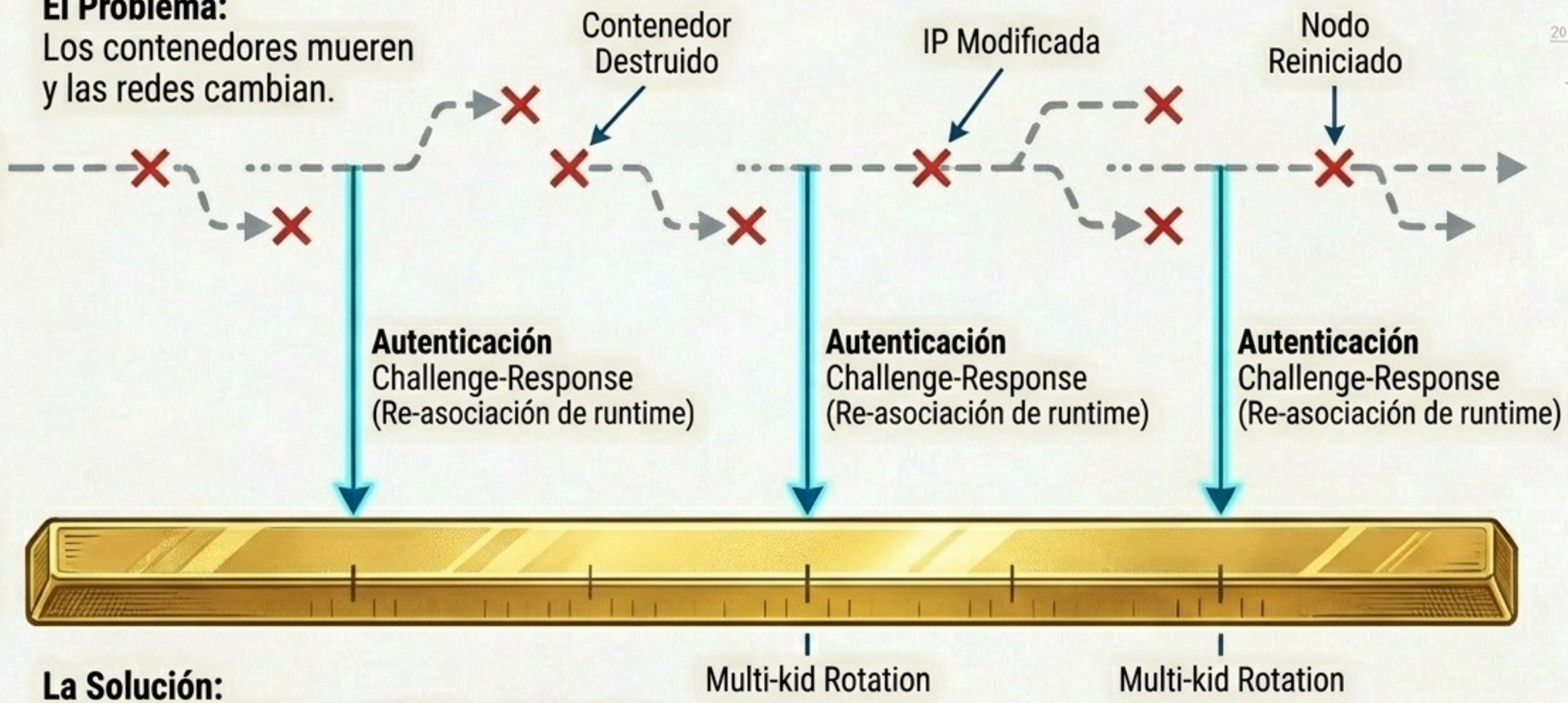
Resiliencia Operacional



1. Emisor firma el payload localmente con su clave privada.
2. Receptor valida la firma RS256 in-memory usando los JWKS precargados.
3. El runtime funcional continúa sin interrupción aunque el Plano de Control sea temporalmente inalcanzable.

Continuidad criptográfica: La identidad sobrevive a la infraestructura

El Problema:
Los contenedores mueren y las redes cambian.



La Solución:
Identidad matemática aislada, con rotación continua sin interrupción de tráfico.

Evolución de la custodia criptográfica por aislamiento progresivo

1 Nivel 1: Custodia Operacional

Claves cargadas temporalmente en memoria runtime (Vault KV). Desacopladas del disco.

2 Nivel 2: Custodia Non-Exportable

La clave privada nunca toca el Engine. Se envía payload y se recibe resultado firmado (Vault Transit).

3 Nivel 3: Hardware-Backed

Claves selladas en hardware criptográfico. Operaciones remotas de firma directa (HSM).

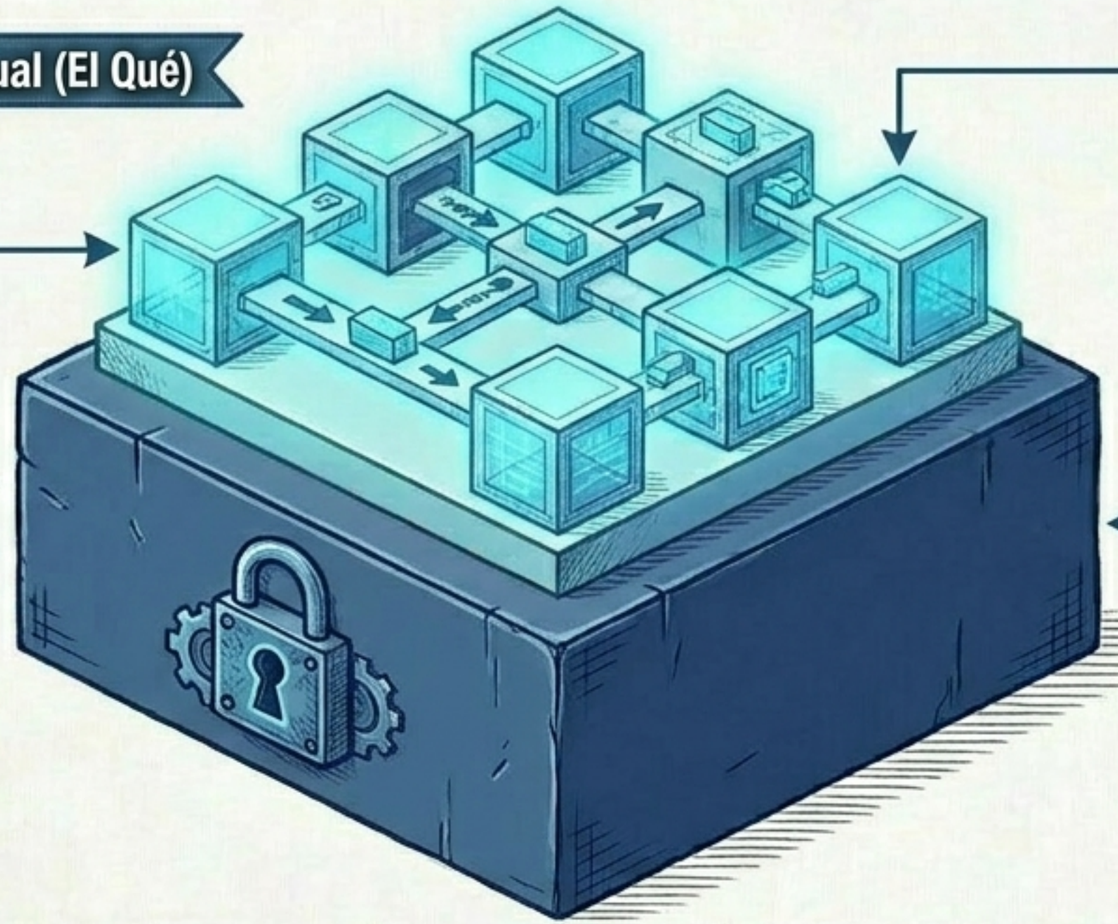
A mayor nivel, el compromiso total del host funcional NO compromete el material criptográfico base.

La confianza abre el canal estructural; el contexto define la acción

Capa 2: Autorización Contextual (El Qué)

¿Puede esta identidad de máquina invocar esta API específica para este Tenant?

Resuelto operacionalmente mediante políticas IAM y contexto.



Capa 1: Confianza Estructural

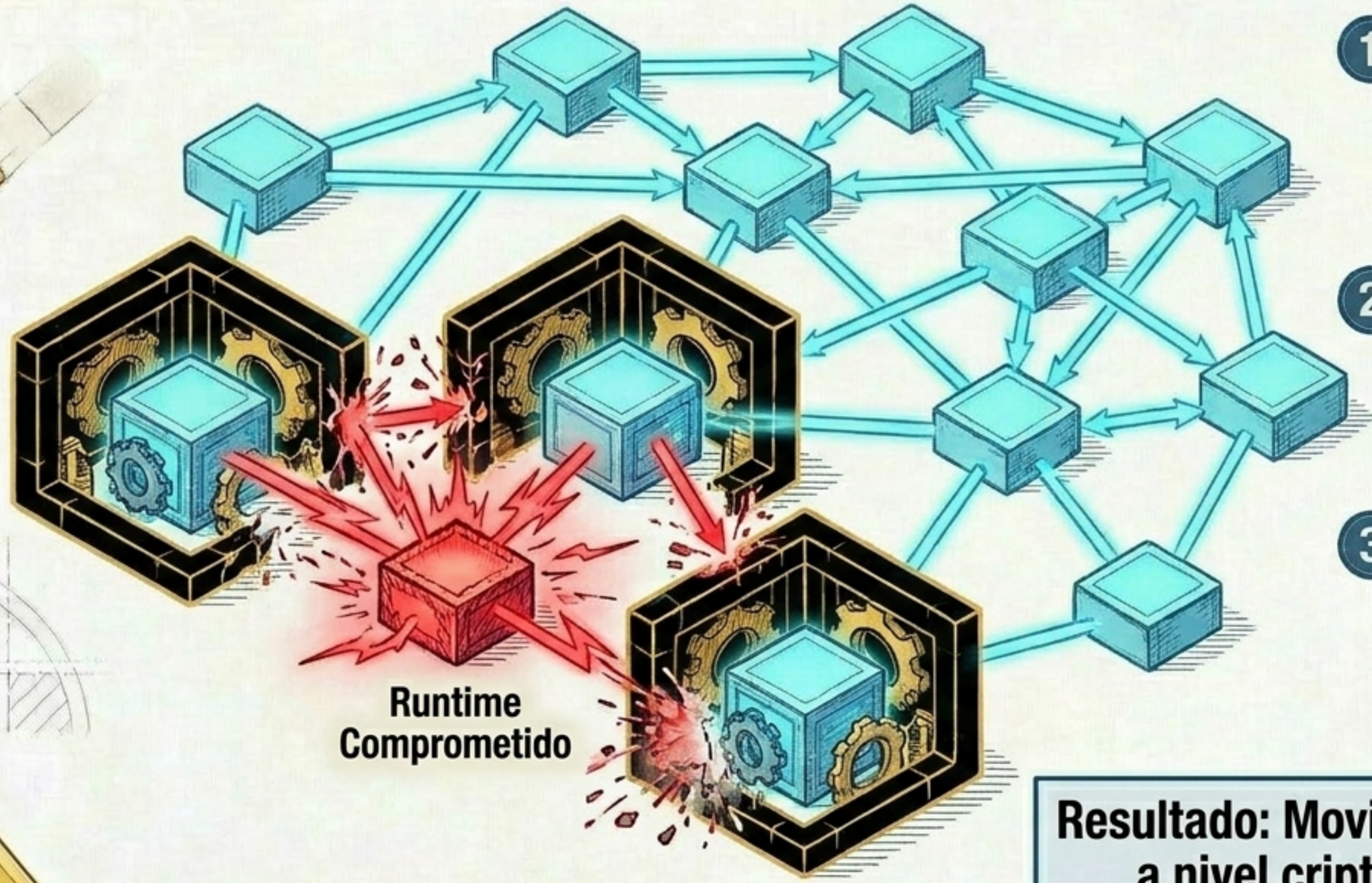
(El Quién)

¿Pueden interactuar el Plano A y la Aplicación B de forma segura?

Resuelto matemáticamente mediante firmas y distribución de JWKS.

Principio de Diseño: Nunca se generan nuevas relaciones criptográficas horizontales (Trust) entre aplicaciones para resolver necesidades de contexto.

Diseño por compartimentación: Conteniendo el Blast Radius



1. Cero Confianza Horizontal

Un Engine comprometido no mantiene “trust bundles” hacia sus vecinos.

2. Aislamiento de Claves

Las claves privadas nunca se comparten. Imposible extraer la identidad de otros nodos.

3. Aislamiento de Custodia

Cero acceso lateral en los sistemas Vault/HSM entre cápsulas.

Resultado: Movimiento lateral bloqueado a nivel criptográfico fundacional.

Validación estratégica: Por qué exigimos un modelo distribuido

	Tradicional / Centralizado	SkyDefended InfraApp
Rendimiento en Runtime	✗ Cuello de botella por latencia síncrona.	✓ Zero latencia de red añadida (validación in-memory).
Disponibilidad Funcional	✗ Dependencia crítica del servidor de Auth.	✓ Resiliencia total; el runtime opera sin el Control Plane.
Escalabilidad	✗ Vertical (Costosa y limitada).	✓ Horizontal, lineal y descentralizada por cápsulas.
Anclaje de Seguridad	✗ Identidad atada a perímetros, IPs o VPNs falibles.	✓ Identidad atada exclusivamente a criptografía aislada.

El Estatus Definitivo de Zero Trust

Materializada mediante identidades RSA y JWKS.

Sobrevive a runtimes efímeros sin latencia.

> **“La confianza en SkyDefended InfraApp es explícita, previa, mediada por el Plano de Control y validada localmente.”**

Jamás depende de redes o infraestructura.

Custodia evolutiva hasta el hardware (HSM).

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS