SkyDefended InfraApp v1.3

Arquitectura Distribuida Zero Trust y Modelo Multi-Plano

| 21 de Mayo de 2026 | Documento de Arquitectura Técnica | Ismael Cruz Casasola

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS

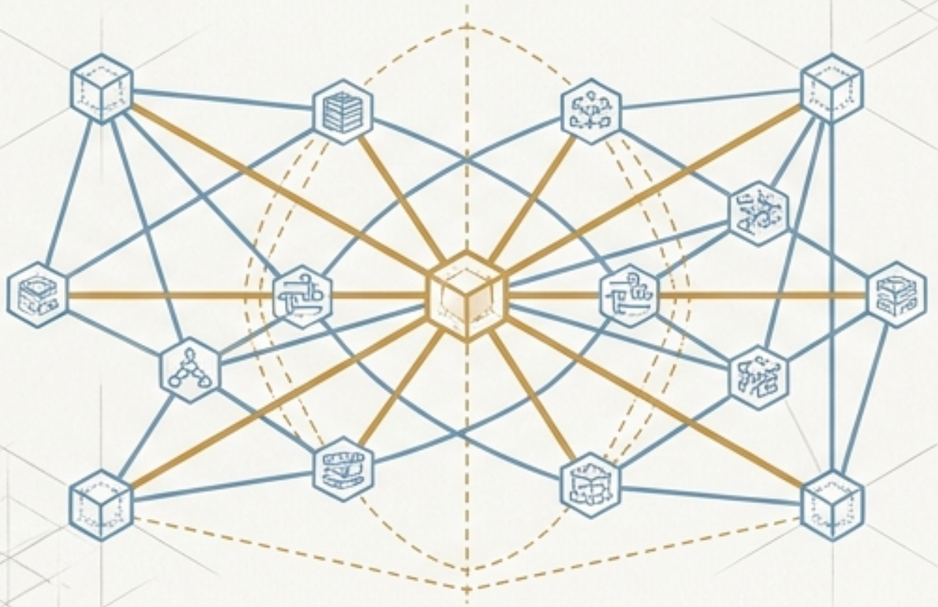
NEGATIVE SPACE

Centralización
de Datos

SkyDefended InfraApp NO centraliza los datos ni la lógica funcional de las aplicaciones. No absorbe el dominio operacional del software.

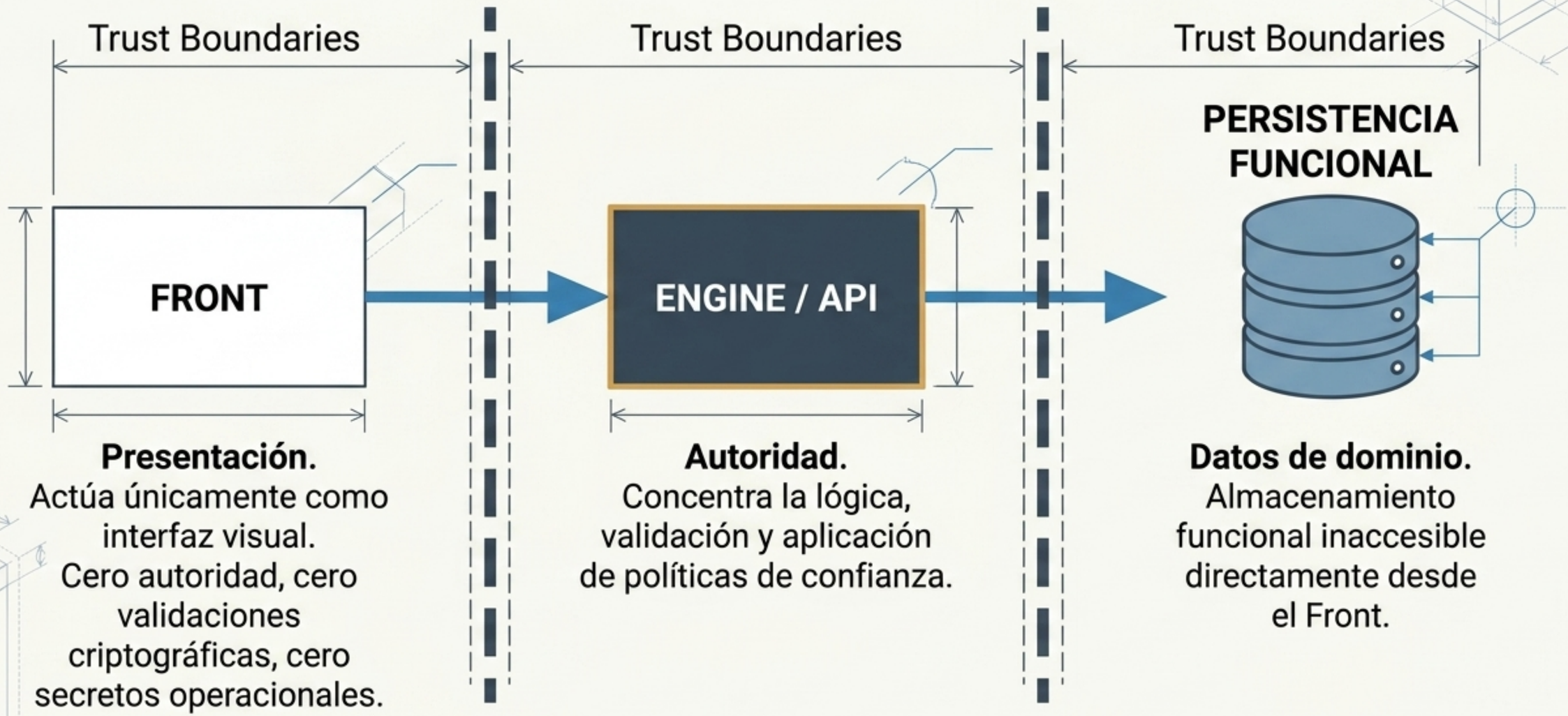
THE CORE AXIOM

Decentralized execution
with centralized policy



Centraliza las condiciones. Gobierna exclusivamente las reglas bajo las cuales el software puede existir, operar e interactuar dentro de un modelo de confianza Zero Trust distribuido.

El Principio Arquitectónico Base

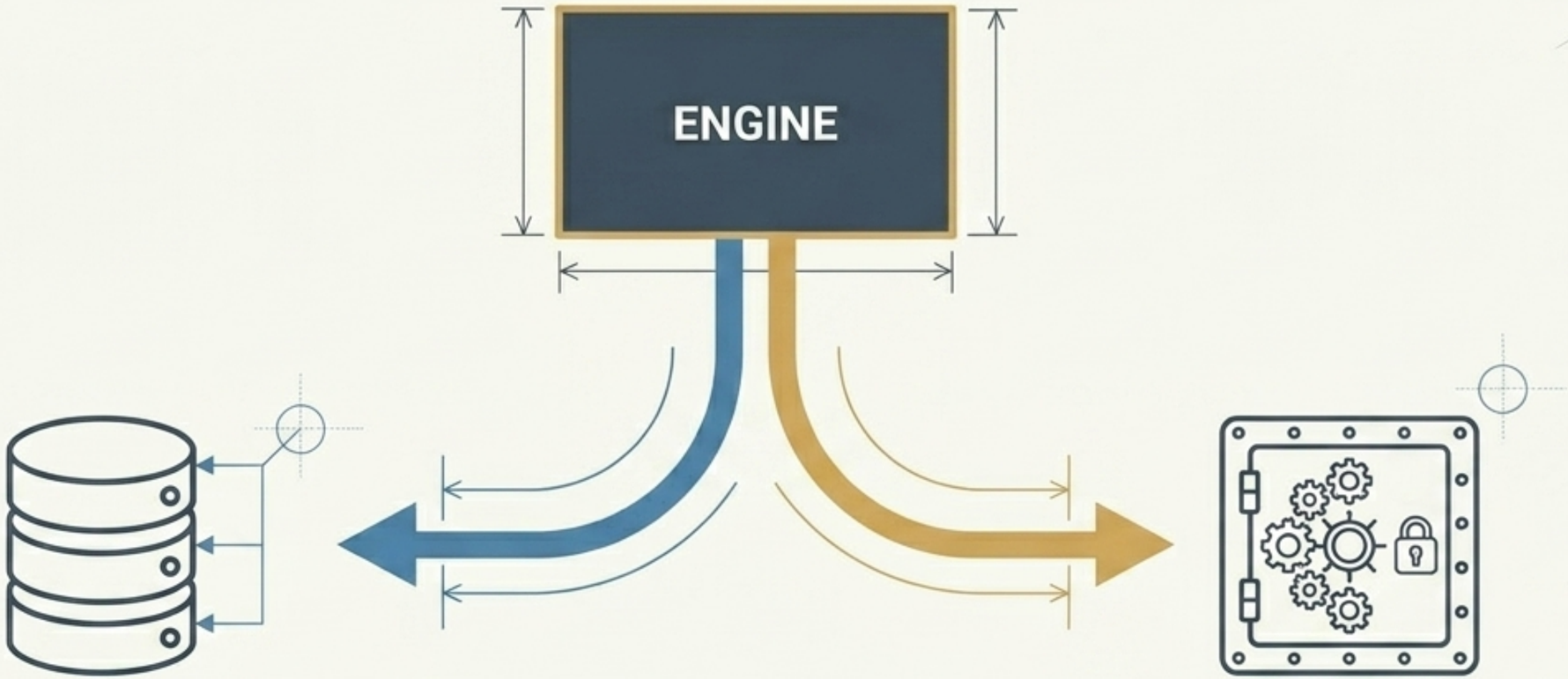


Presentación.
Actúa únicamente como interfaz visual. Cero autoridad, cero validaciones criptográficas, cero secretos operacionales.

Autoridad.
Concentra la lógica, validación y aplicación de políticas de confianza.

Datos de dominio.
Almacenamiento funcional inaccesible directamente desde el Front.

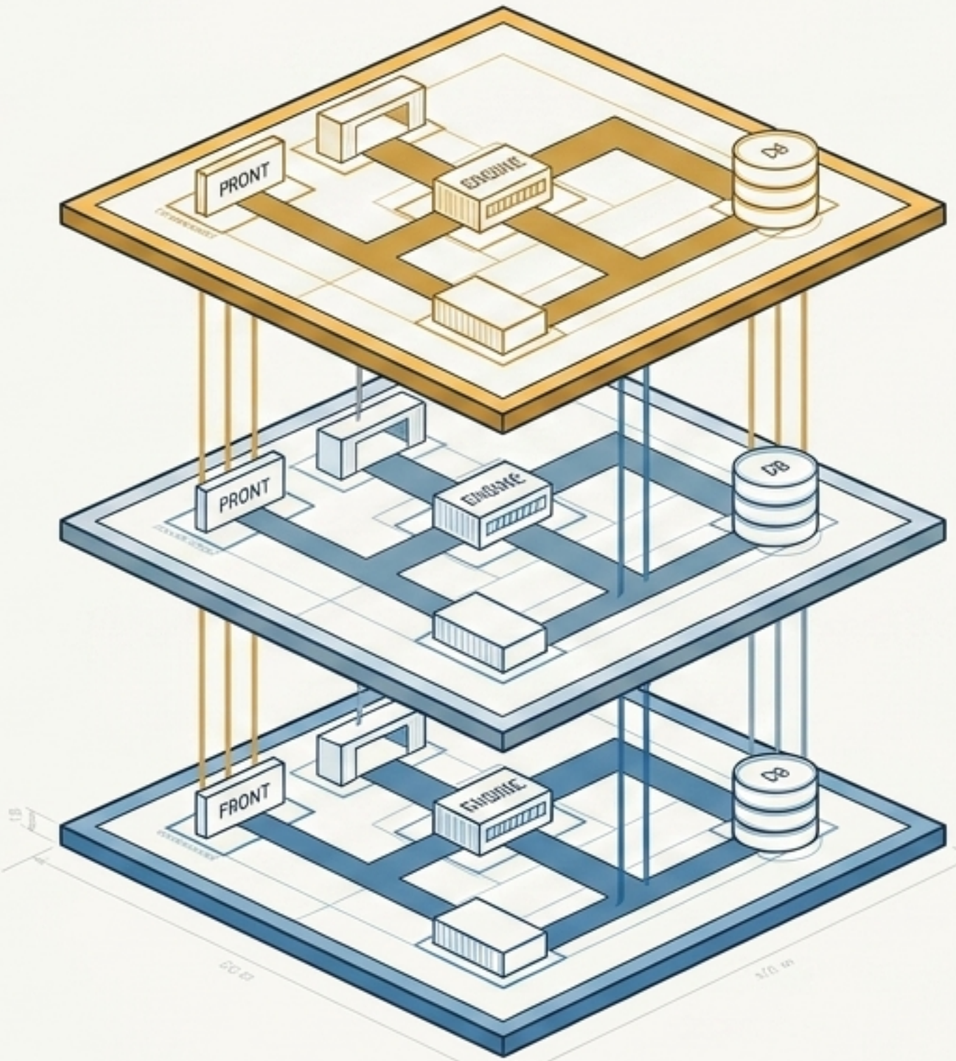
Separación del Modelo de Persistencia



Persistencia Funcional
Almacena datos operativos, estado y configuración. (Dominio Funcional).

Persistencia Criptográfica Desacoplada
Custodia de identidades, material criptográfico y secretos. Nunca almacenados en BBDD funcionales ni en memoria efímera de runtime. (Dominio de Confianza).

El Modelo de Tres Planos



Plano de Control

Control (FRONT → ENGINE → DB). Establece la pertenencia, define los Policy Bundles y emite la confianza criptográfica raíz.

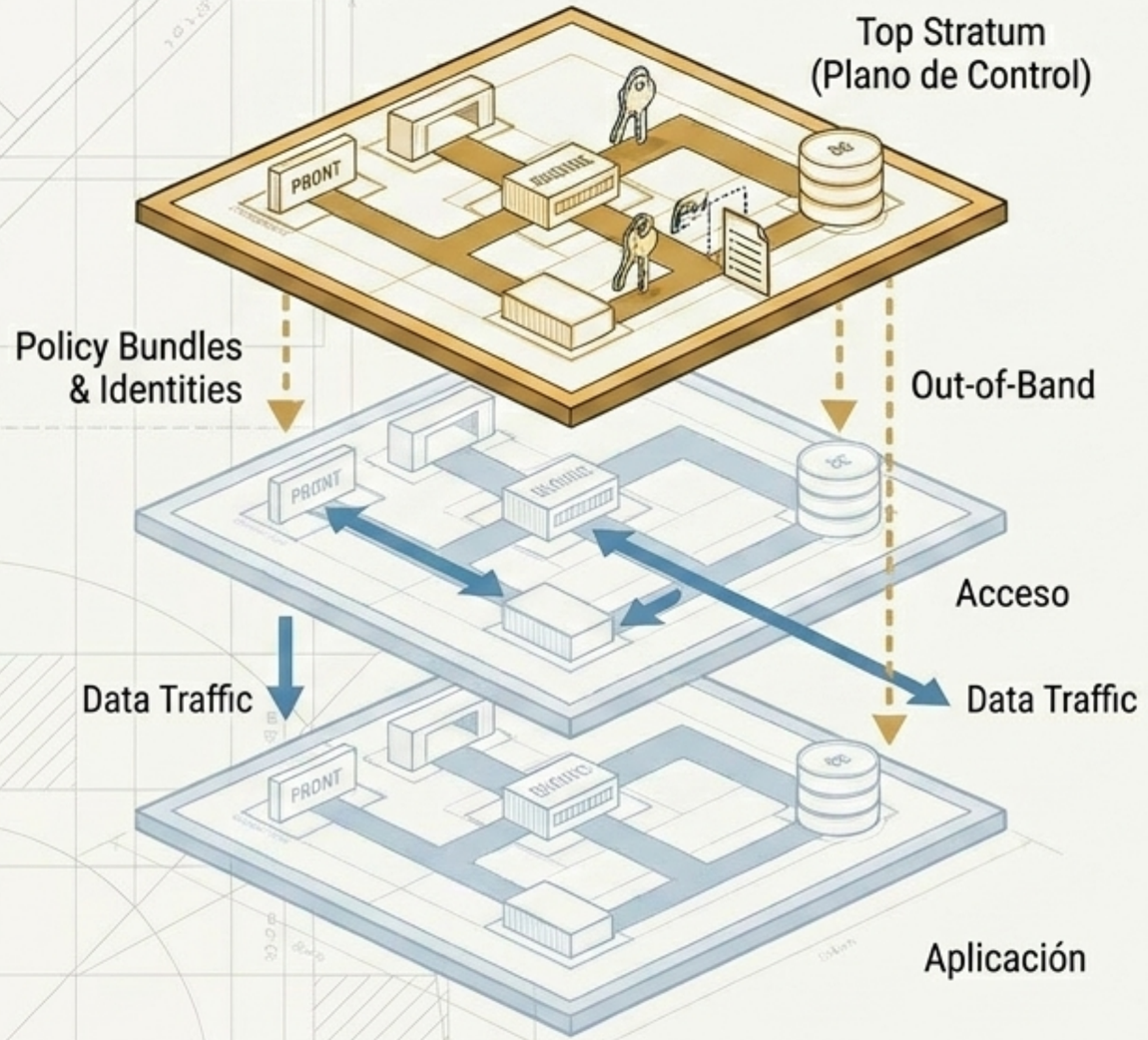
Plano de Acceso

Acceso (FRONT → ENGINE → DB). Punto único de entrada y administración unificada del tenant. Entorno operativo del cliente.

Plano de Aplicación

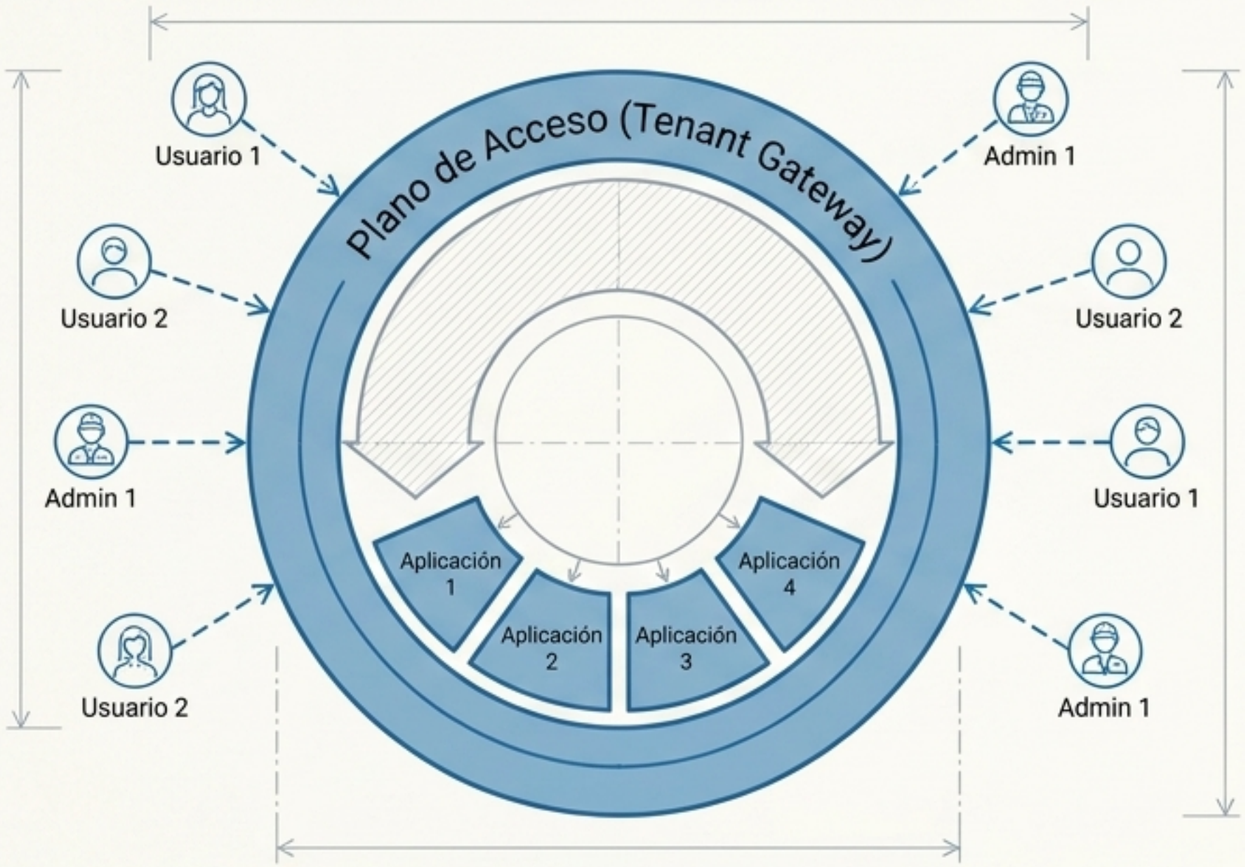
Aplicación (FRONT → ENGINE → DB). Ejecución funcional, lógica de negocio y custodia de datos independientes.

Plano de Control: Root of Trust



Qué ES	Qué NO ES
• Root of Trust.	• No es un plano de datos.
• Registros de pertenencia (Tenants, Licencias).	• Fuera del data path de las aplicaciones.
• Registros de confianza (Identidades criptográficas, Policy Bundles).	• No posee claves privadas operativas de los Engines inferiores.
• Operado íntegramente por NCN.	• No ejecuta lógica funcional.

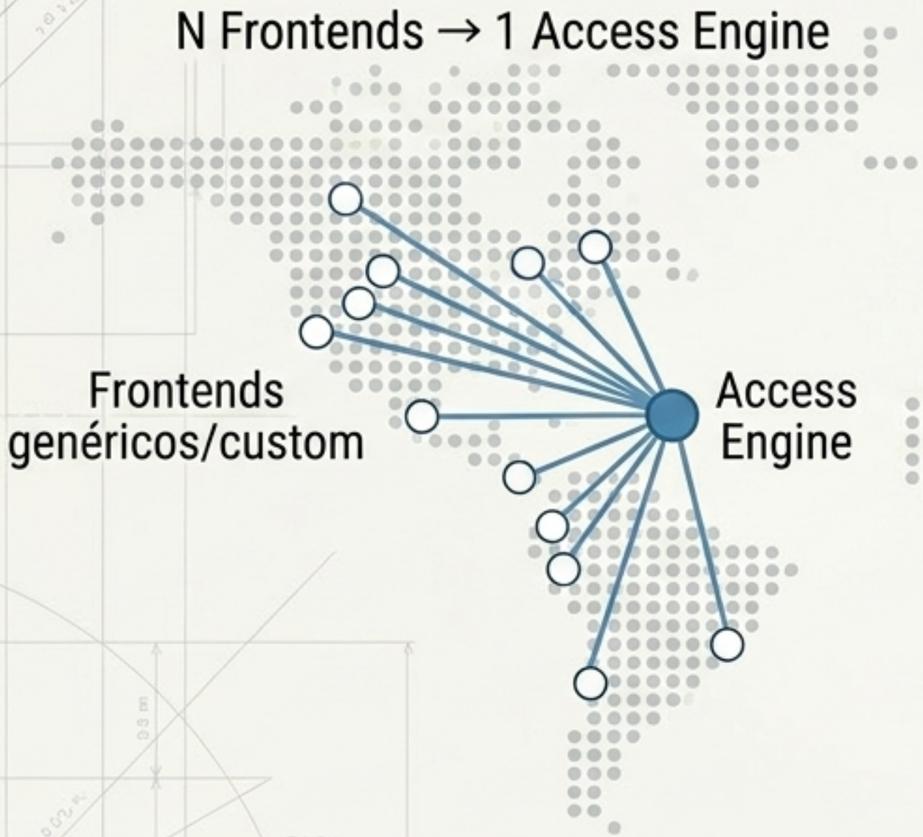
Plano de Acceso: Tenant Gateway

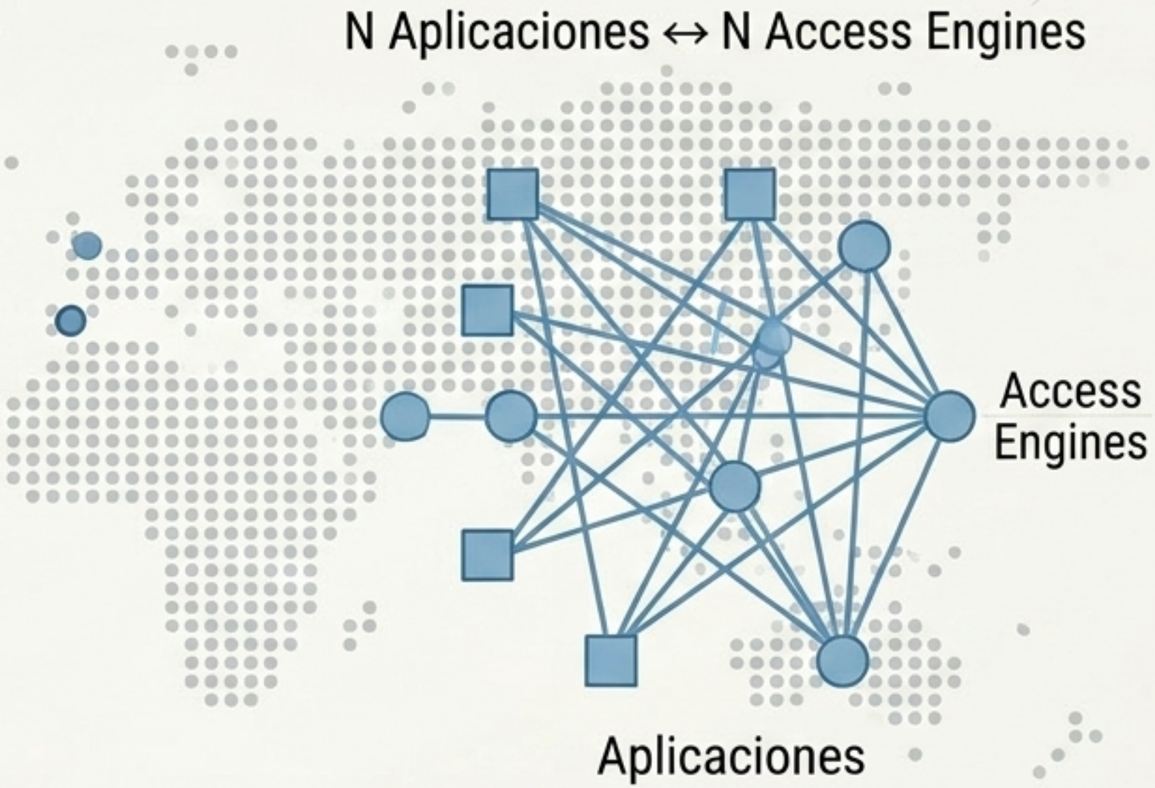


El shell administrativo unificado del tenant. Instancia identidades, sesiones, políticas de entrada y contexto operativo.

Regla Estructural: Unifica la experiencia administrativa y el control de acceso, pero NO define la lógica de negocio ni gobierna los datos internos de los productos.

Independencia Topológica y Relaciones Distribuidas

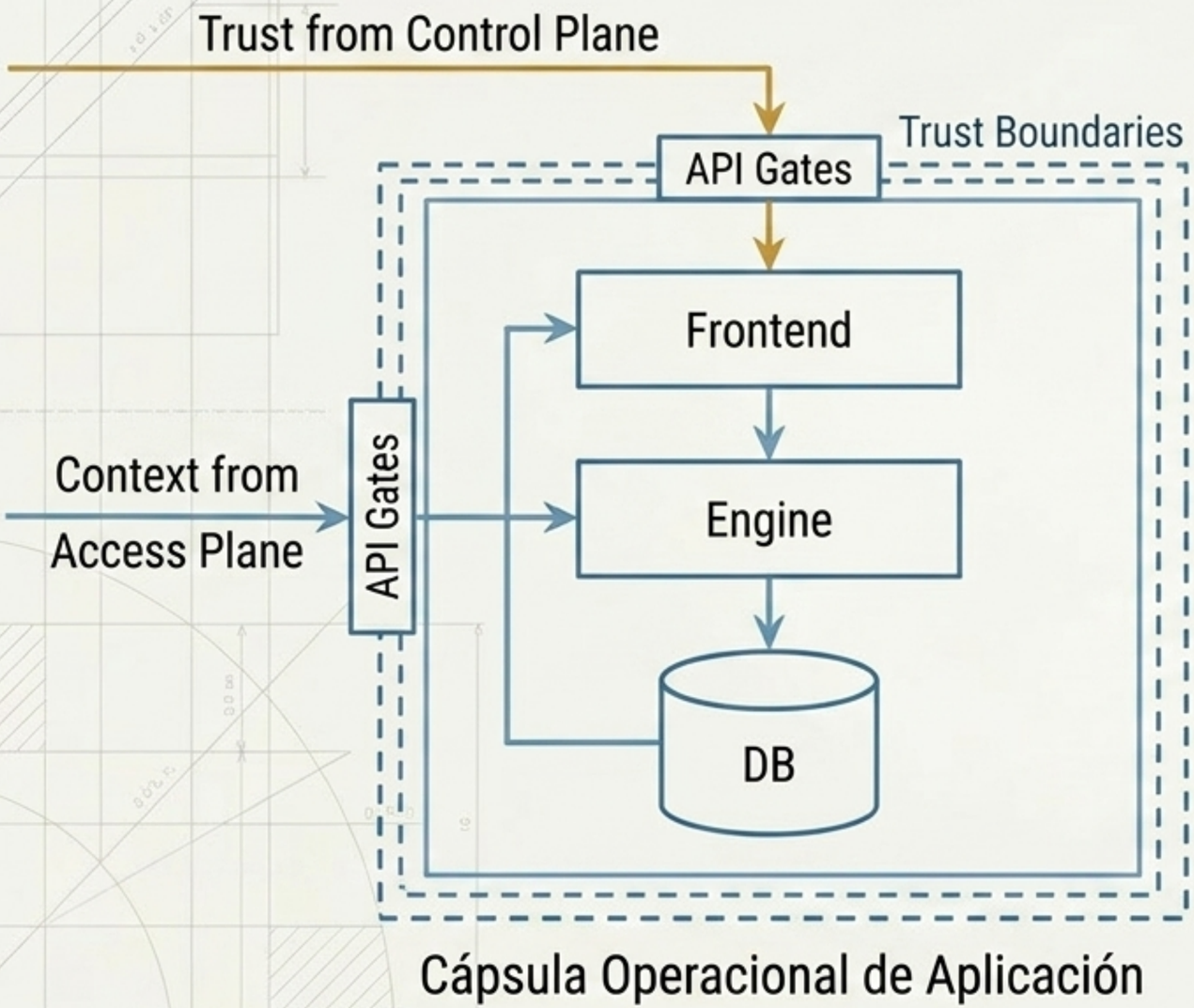




Independencia Topológica: Frontends genéricos o con branding personalizado (N) apuntan a la misma autoridad (1 Engine).

Las aplicaciones se conectan al Plano de Acceso sin ataduras a una instancia física o geográfica concreta.

Plano de Aplicación: La Cápsula Operacional

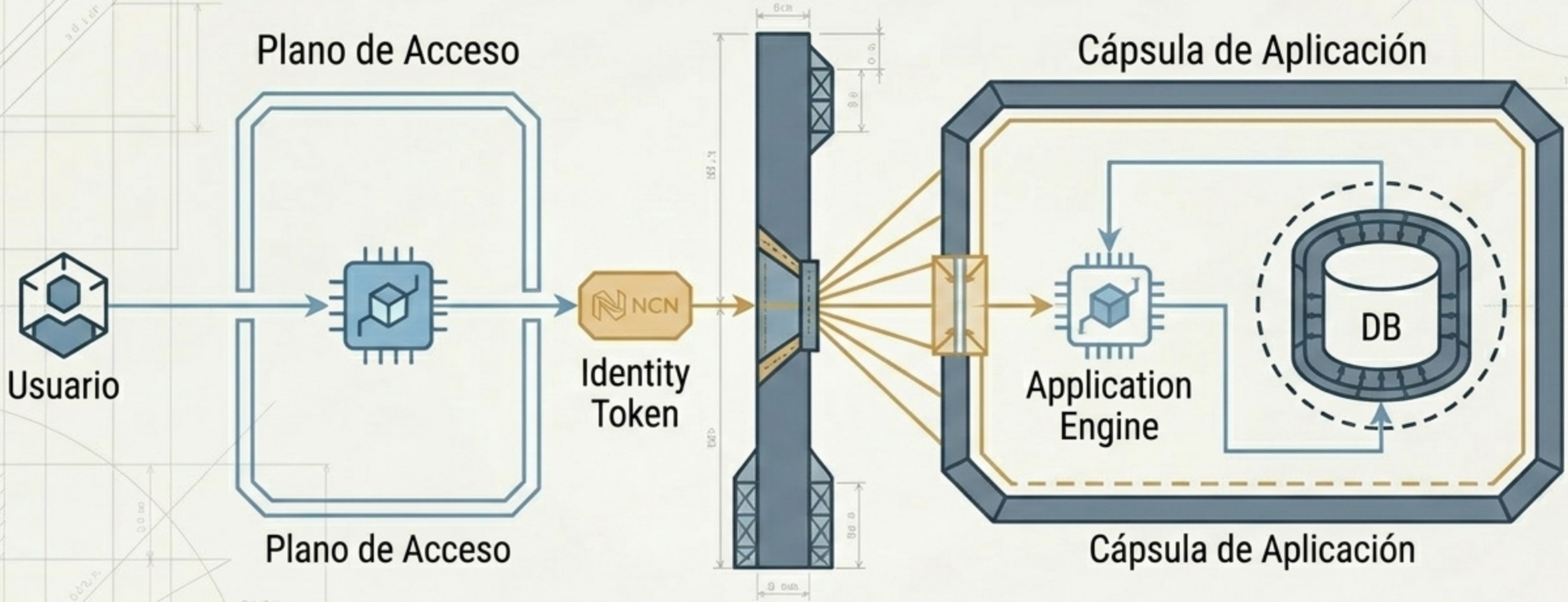


Autonomía Funcional Total: La aplicación mantiene su propio modelo de datos, lógica y reglas internas.

Validación Local: Verifica la confianza mediante Policy Bundles sin depender de llamadas síncronas al Plano de Control.

Frontends Adicionales: Capacidad de exponer portales públicos independientes fuera del shell administrativo.

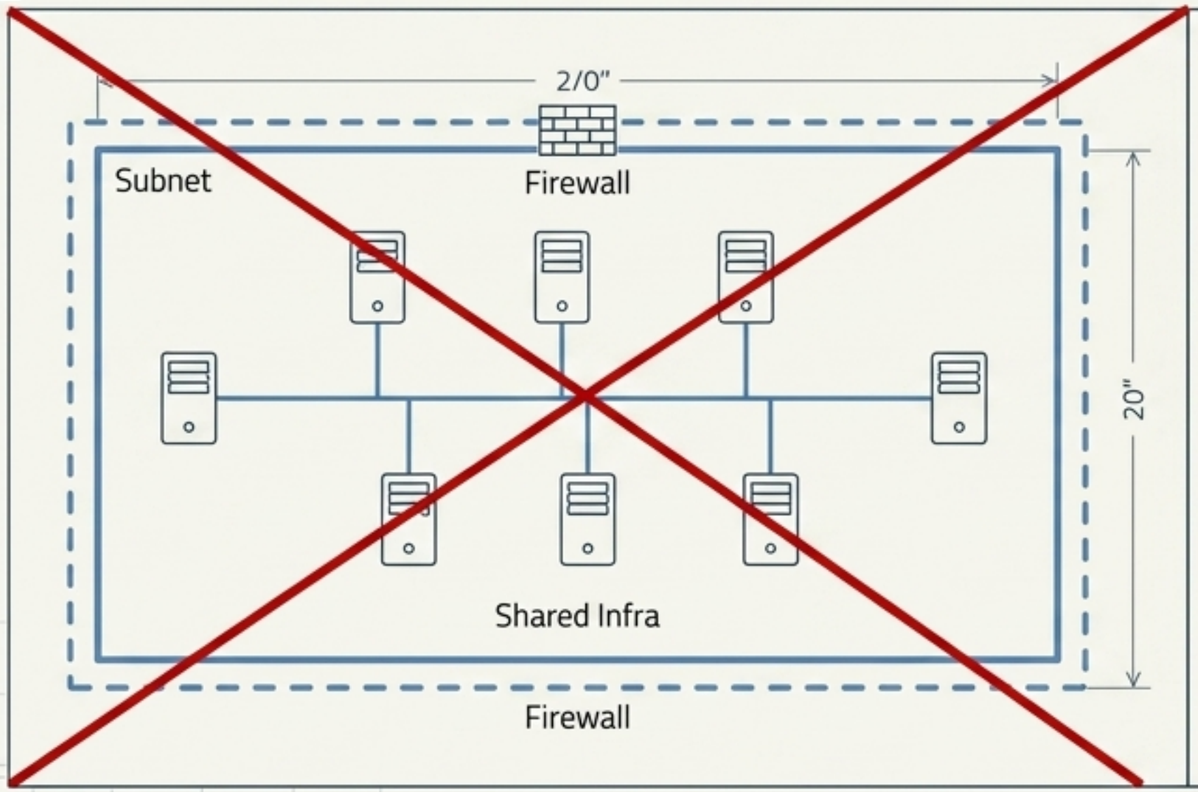
Integración sin Absorción



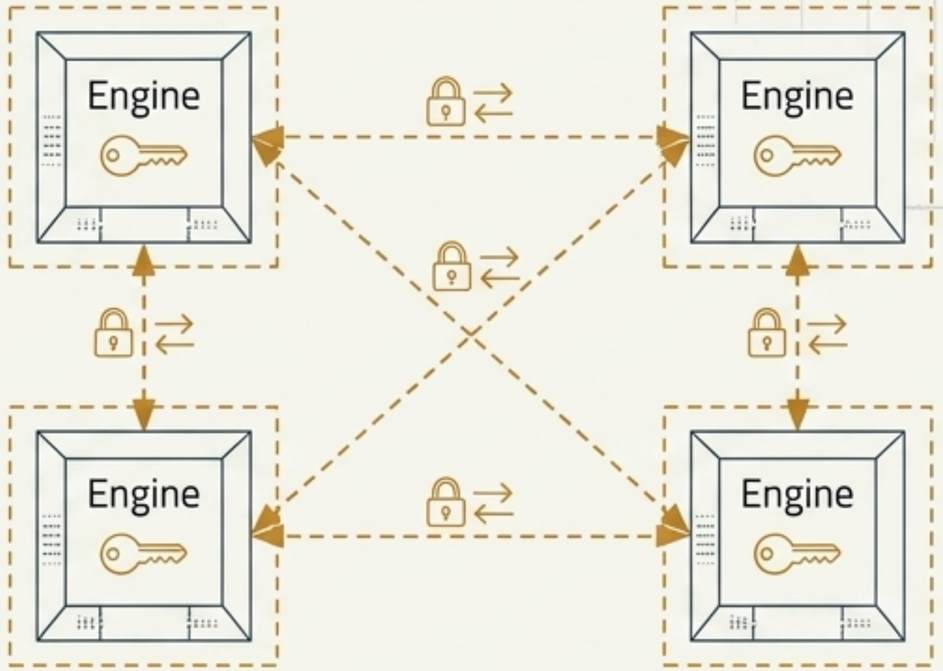
- El usuario interactúa en el entorno administrativo unificado del tenant.
- El Plano de Acceso transporta identidad y contexto.
- La persistencia, el procesamiento interno y los datos permanecen estrictamente encapsulados en el dominio de la aplicación.

Mecánicas de Confianza: Trust Boundaries Distribuidos

Confianza Implícita (Subred/Proximidad)



Confianza Criptográfica Distribuida

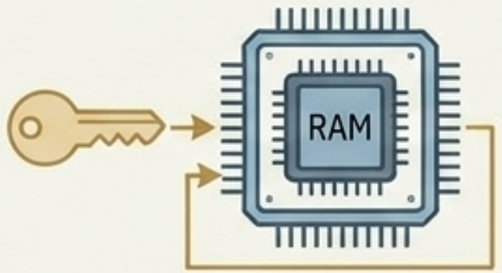


Trust Boundaries Distribuidos. La confianza no reside en infraestructura compartida, proximidad topológica o sesiones de usuario.

Identidad Asociada a Engines. Cada Engine posee una identidad criptográfica persistente, validada localmente mediante mecanismos Zero Trust.

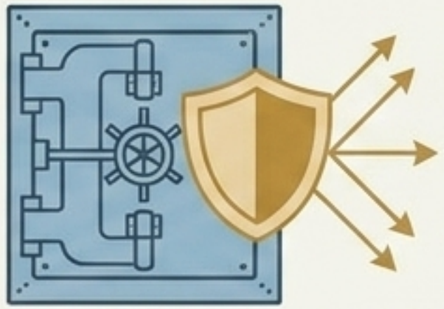
Evolución de la Custodia Criptográfica

Nivel 1 (Vault KV)



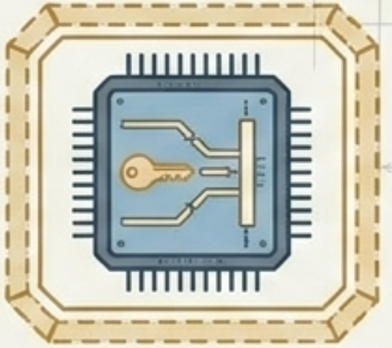
Persistencia desacoplada.
Carga temporal en memoria runtime.

Nivel 2 (Vault Transit)



Custodia non-exportable.
El runtime solicita operaciones sin acceso directo a la clave.

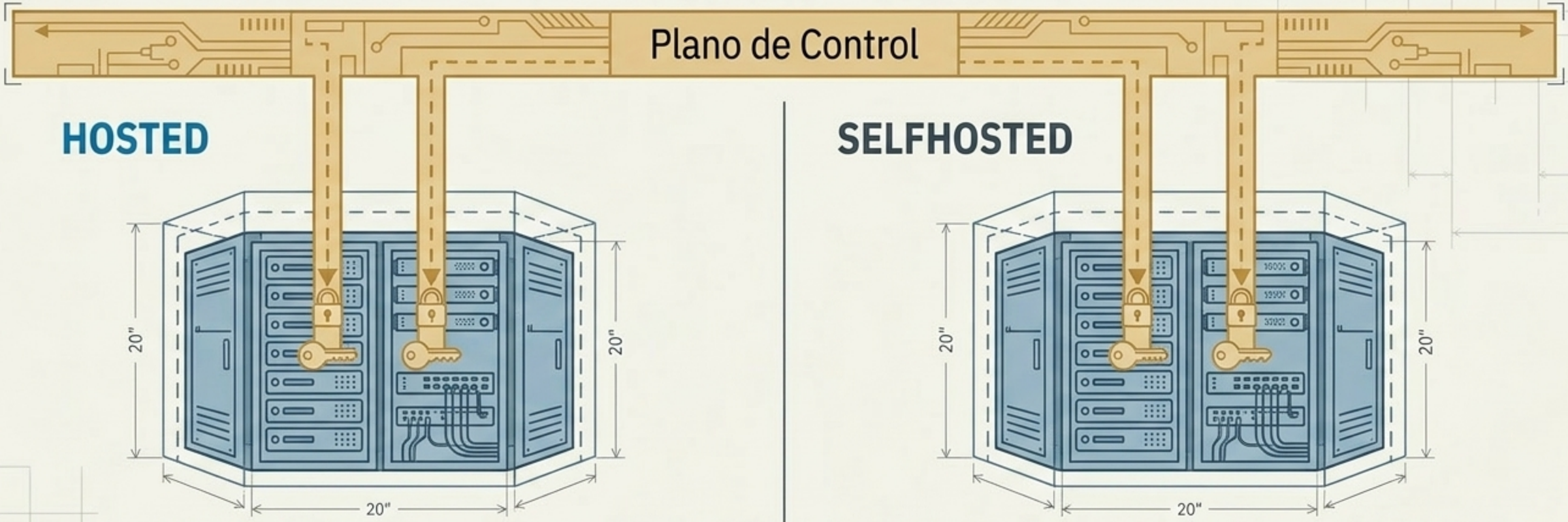
Nivel 3 (HSM remote-sign)



Custodia hardware-backed.
La clave privada nunca abandona el módulo dedicado.

Objetivo estructural: Desacoplar progresivamente las operaciones criptográficas del runtime efímero.

Modelos Operativos y Resiliencia Topológica

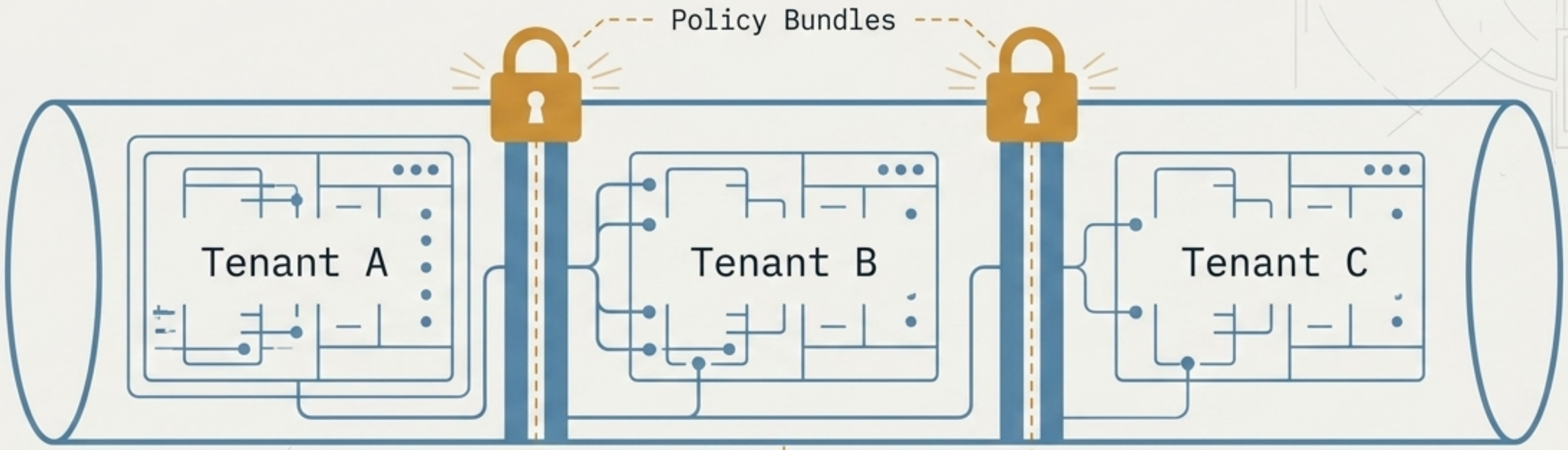


Operado por NCN (Infraestructura, runtime, networking). Autonomía de datos mantenida.

Operado por Cliente/Tercero (Soberanía física, cumplimiento regulatorio).

En ambos modelos, el Plano de Control continúa distribuyendo confianza y el tenant mantiene integración completa sin fracturar la topología de seguridad.

Aislamiento Multi-Tenant en Infraestructura Compartida



Coexistencia sobre infraestructura compartida con aislamiento criptográfico y operativo.

Separación lógica garantizada mediante Policy Bundles distribuidos.

Identidades criptográficas independientes por contexto.

Cero confianza implícita inter-tenant; toda interacción requiere habilitación explícita en el Plano de Control.

Síntesis Arquitectónica: SkyDefended InfraApp

Axioma Estructural.

(FRONT → ENGINE → Persistencia).
Separación inquebrantable de presentación y autoridad.

Tres Planos.

(Control, Acceso, Aplicación).
Separación de pertenencia, administración y ejecución.

Gobernanza unificada. Autonomía absoluta de datos.

Identidad Zero Trust.

Confianza fundamentada en persistencia criptográfica desacoplada, nunca en proximidad o red.

Integración sin Absorción.

Las aplicaciones se integnción.
Las aplicaciones se integran en el shell del tenant sin sacrificar su soberanía funcional o topológica.