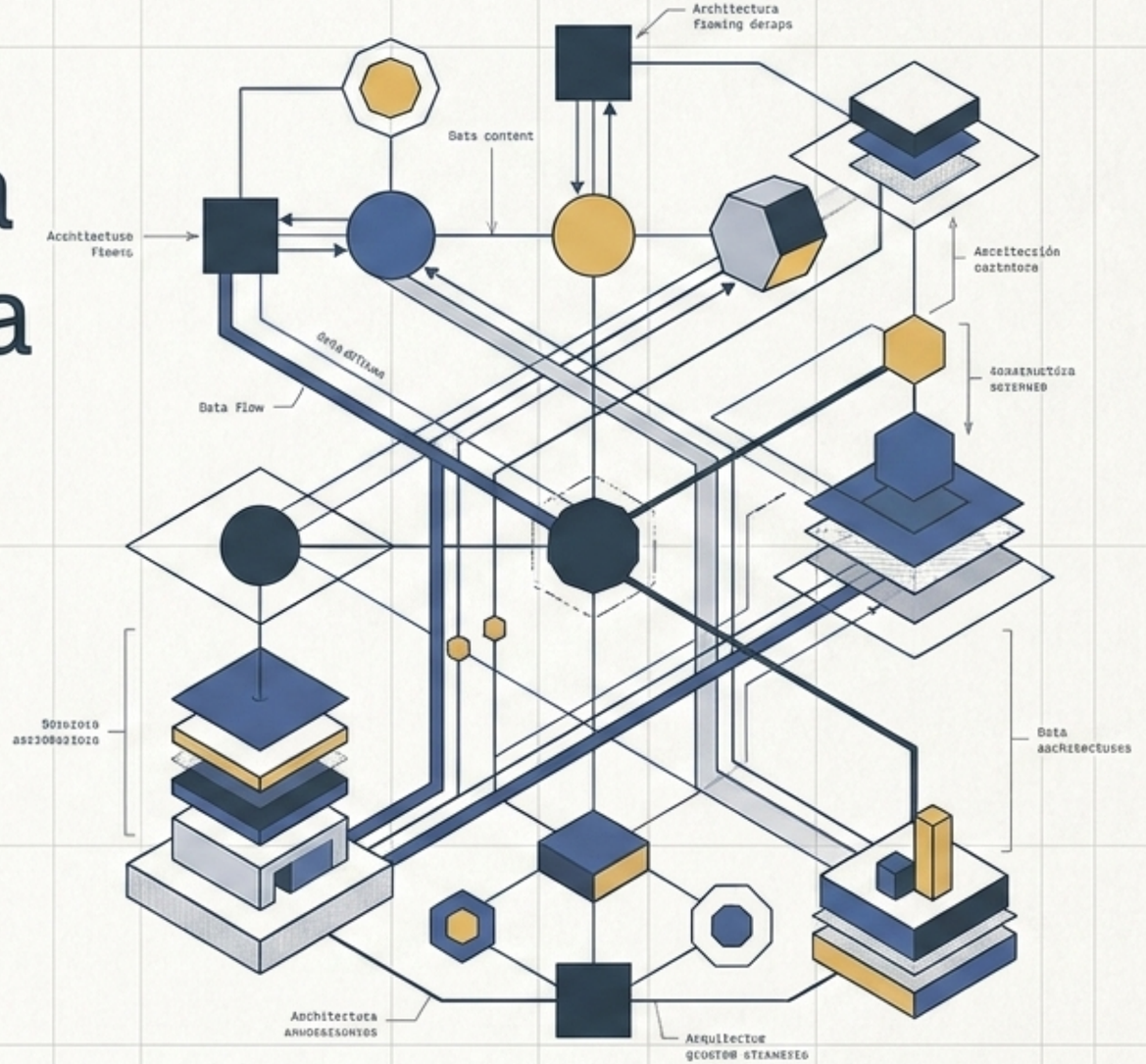
Modelo de Gobernanza Autorizativa Distribuida

Arquitectura Zero Trust Multi-Plano en SkyDefended InfraApp (v1.1)

Documento: D06 - IAM + PIM + ABAC
Autor: Ismael Cruz Casasola



NEXOCYBER NETWORKS
NETWORKING, SEGURIDAD Y SISTEMAS

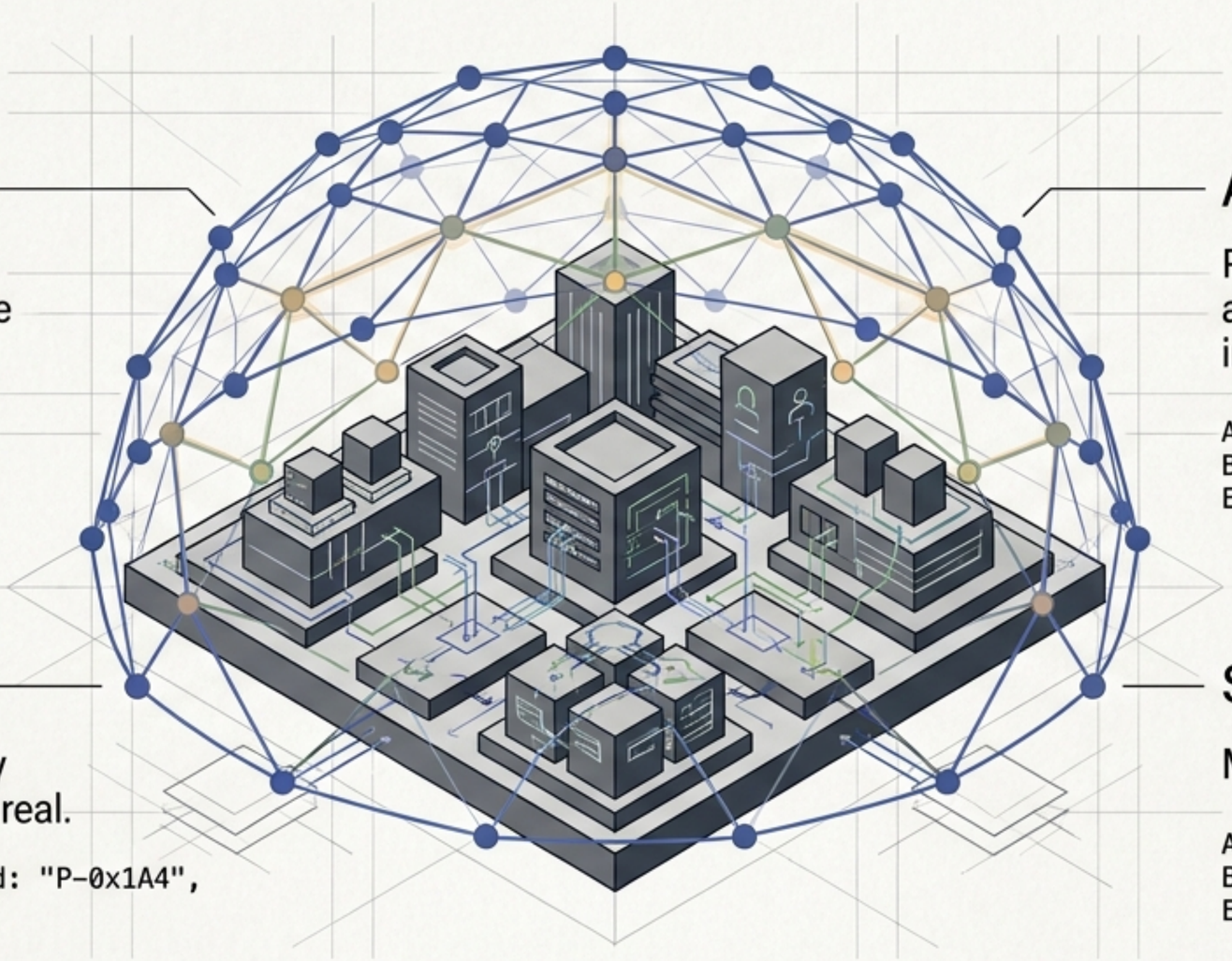
El Paradigma de la Soberanía Autorizativa

SkyDefended InfraApp implementa una capa soberana de gobernanza autorizativa distribuida construida sobre confianza criptográfica explícita.

Identity-Centric

La autorización sigue a la identidad criptográficamente validada.

```
PKI_VALIDATED: true;
ASSERTION_BOUND: user_did
```



Application Autonomy

Proporciona la capa administrativa unificada sin invadir la lógica de negocio.

```
ADMIN_LAYER: unified_control;
BUSINESS_LOGIC: untouched;
ENFORCEMENT: decentralized
```

Context-Aware

Validación local distribuida y evaluación ABAC en tiempo real.

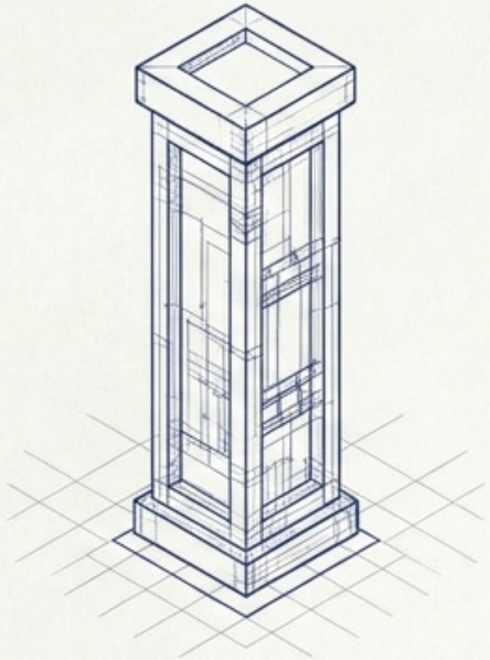
```
LOCAL_POLICY_EVAL: {policy_id: "P-0x1A4",
timestamp: "T-NOW",
risk_level: "LOW"}
```

Sovereign Shield

Multi-tenant ecosystem

```
ADMIN_LAYER: unified_control;
BUSINESS_LOGIC: untuched;
ENFORCEMENT: decentralized
```

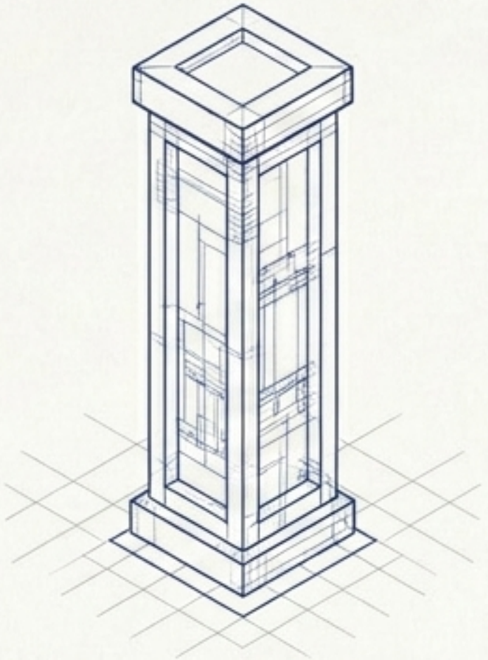
Desacoplando el Acceso: La Tríada Zero Trust



Autenticación (Identidad)

Pregunta: ¿Quién eres?

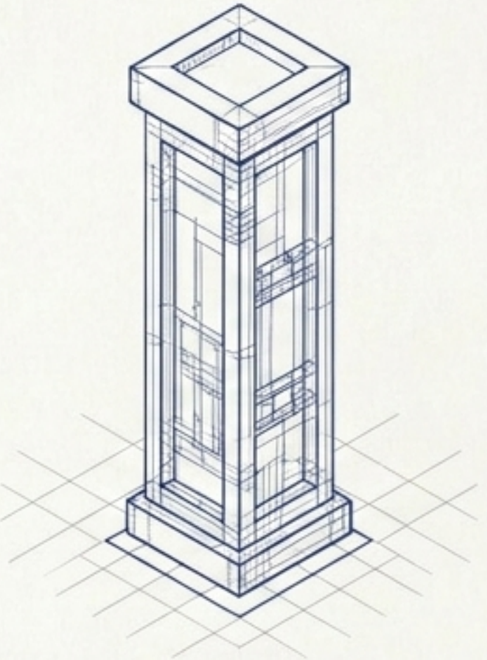
Mecanismo: Identidad válida, credenciales, OIDC.



Confianza Criptográfica (D02)

Pregunta: ¿Podemos relacionarnos?

Mecanismo: Firmas RSA, JWKS, Trust Bundles, Engines.

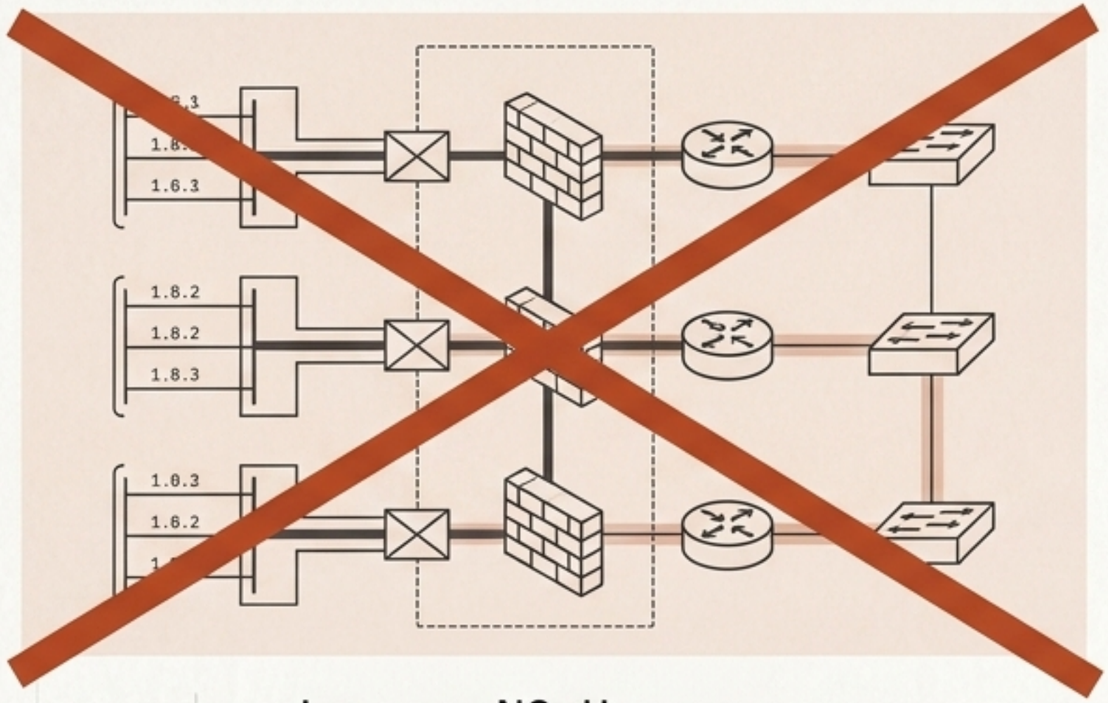


Autorización (D06)

Pregunta: ¿Qué puedes hacer en esta relación?
Mecanismo: Permisos explícitos, IAM, PIM, validación local.

La confianza criptográfica y la autorización representan capas estrictamente distintas del sistema.

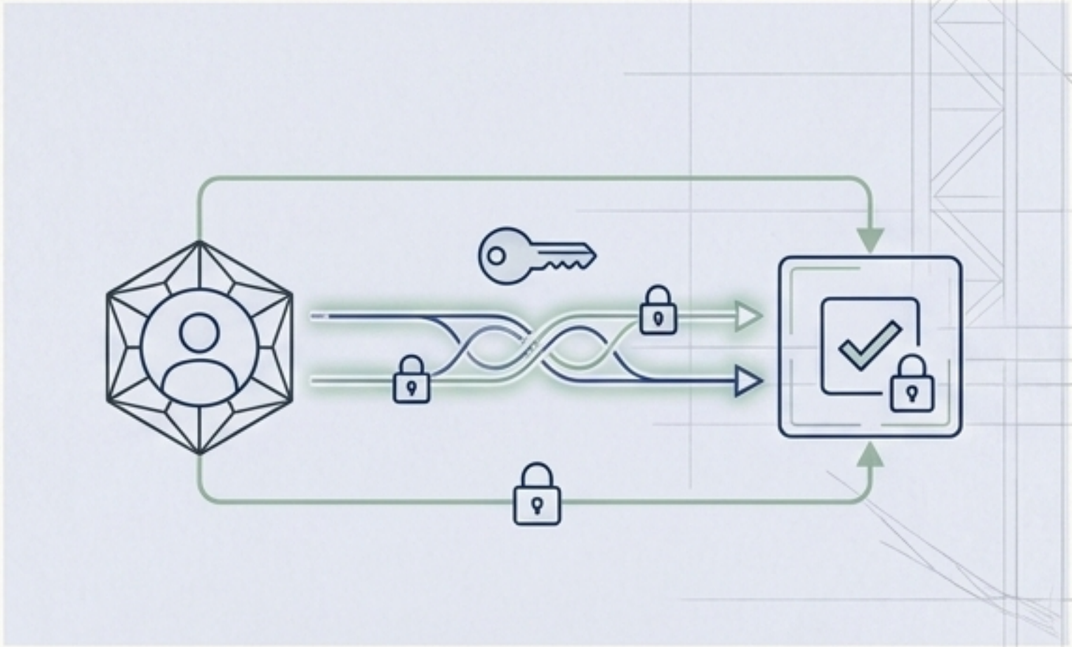
Principios Zero Trust: Vectores de Decisión



Lo que NO Hacemos

SkyDefended InfraApp NO basa autorización en:

- Red o subredes.
- Cluster o infraestructura compartida.
- Proximidad topológica.
- IP o localización física.

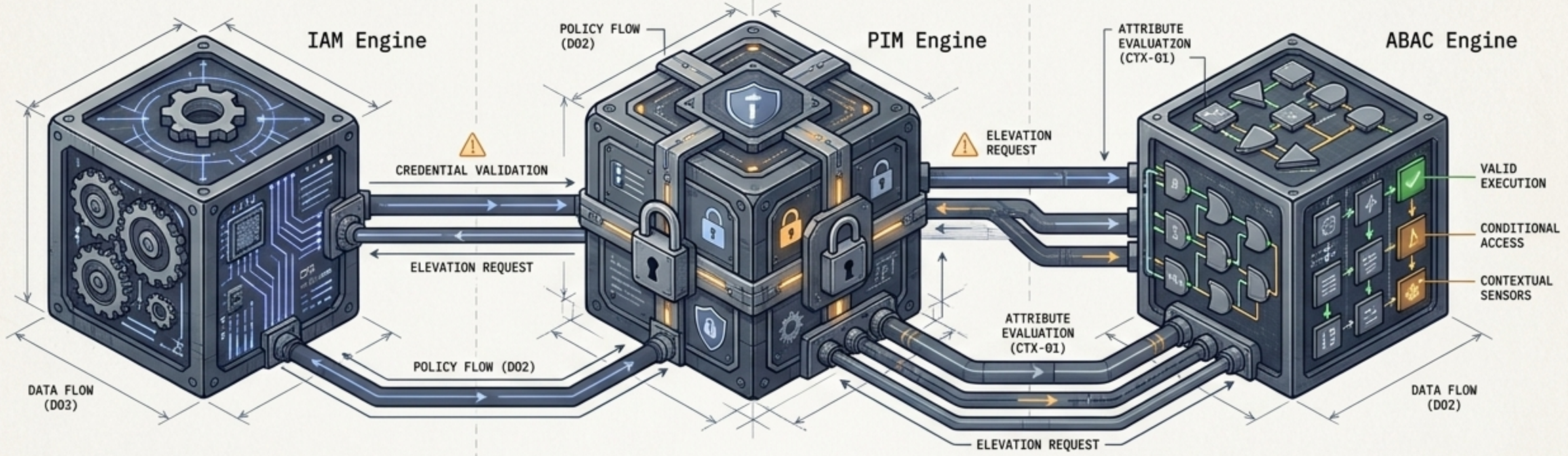


Lo que SÍ Hacemos

La autorización siempre deriva de:

- Identidad explícita.
- Capacidad autorizativa declarada.
- Contexto.
- Relaciones autorizadas criptográficamente.
- Validación local.

Motores de Gobernanza: IAM, PIM y ABAC



IAM (Identity & Access Management)	PIM (Privileged Identity Management)	ABAC (Attribute-Based Access Control)
Naturaleza: Capacidad estructural persistente.	**Naturaleza:** Elevación temporal contextual.	**Naturaleza:** Restricción contextual.
Propósito: Operación diaria, automatización, roles base.	**Propósito:** Operaciones críticas, cambios destructivos, auditoría.	**Propósito:** Definir bajo qué condiciones opera una capacidad ya autorizada.
Duración: Permanente.	**Duración:** Limitada (con expiración automática).	**Mecanismo:** Reglas sobre bindings y roles.

Topología de Aislamiento: Control vs. Acceso

Plano de Control

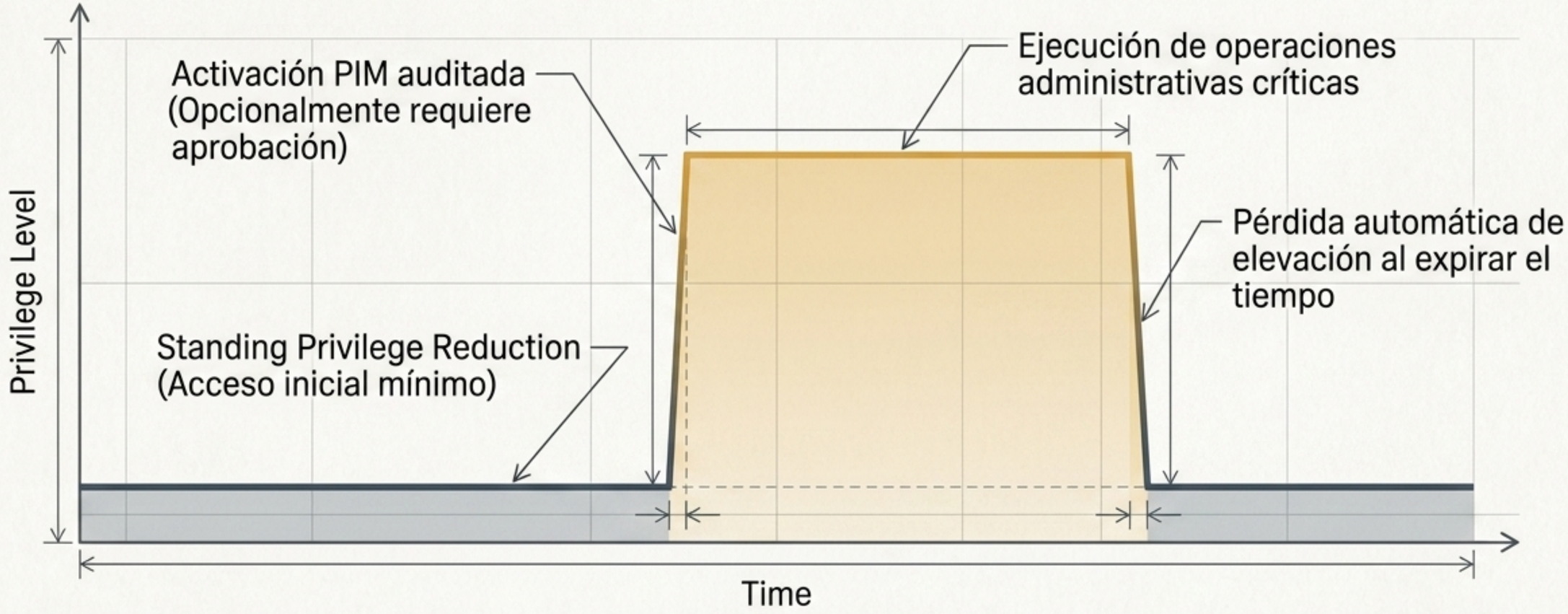
Características Clave
▪ **Gobierna:** Root of Trust de la plataforma, operadores, sincronización autorizativa.
▪ **Excluye:** Tenants, lógicas de negocio funcionales.
▪ **Modelo:** PIM-First (Prioridad de elevación temporal).

FRONTERA DE CONFIANZA

Plano de Acceso

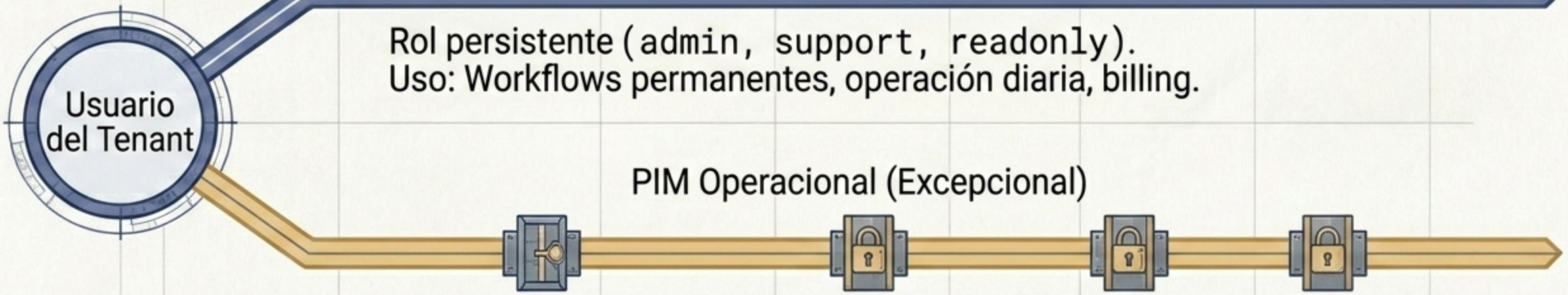
Características Clave
▪ **Gobierna:** Tenants, usuarios funcionales, administración de aplicaciones.
▪ **Modelo:** Híbrido (IAM operacional persistente + PIM para ops. sensibles).

Plano de Control: Arquitectura PIM-First



Los roles IAM permanentes se reservan para automatización e identidades máquina. La operación administrativa humana ocurre exclusivamente mediante elevación temporal PIM.

Plano de Acceso: Gobernanza Híbrida Operacional

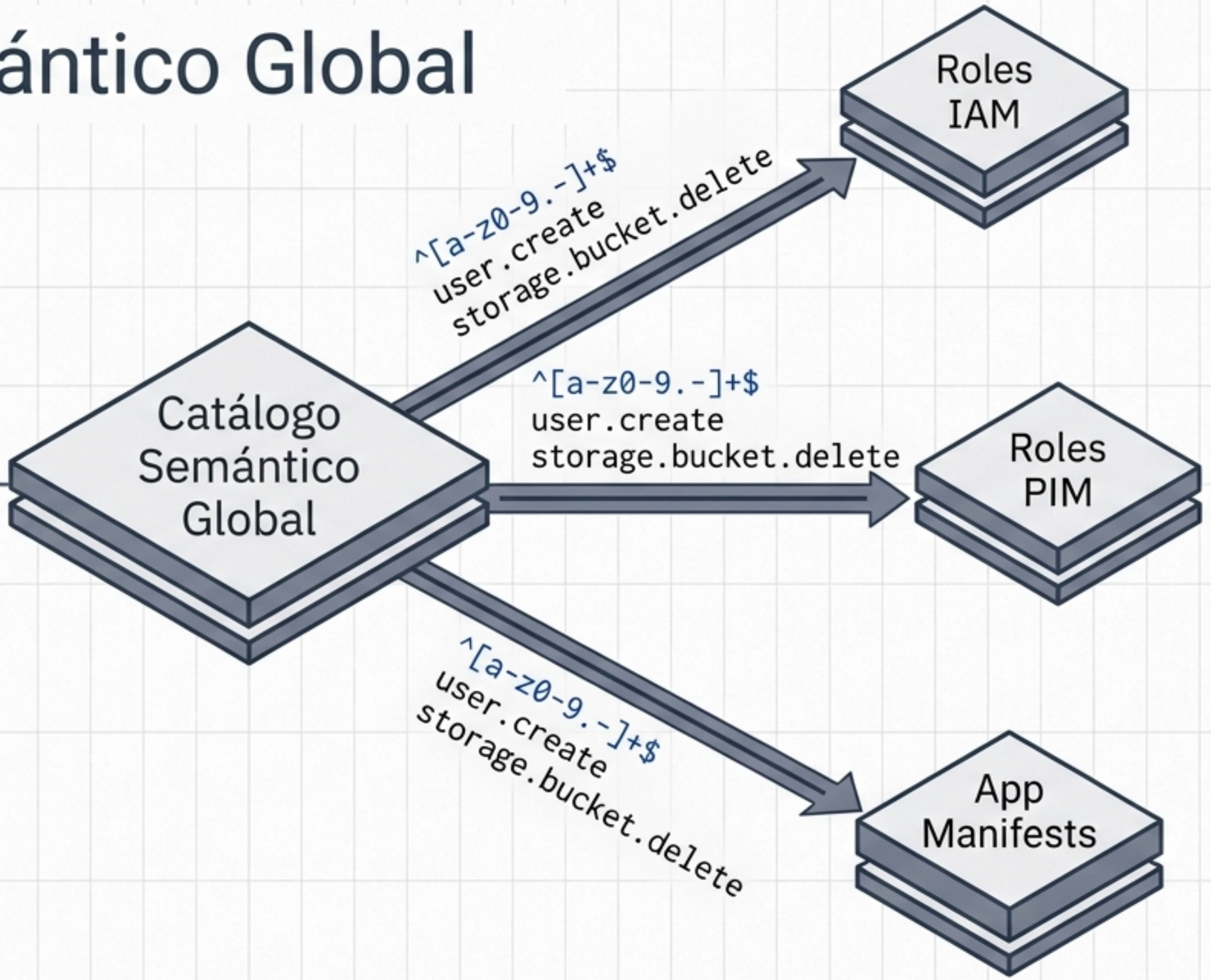


Los usuarios mantienen uno o varios roles IAM persistentes, con cero o varios roles PIM asignables temporalmente.

El Catálogo Semántico Global

Identidad Semántica Global: Los permisos se identifican por slugs únicos (ej. `user.create`, `storage.bucket.delete`).

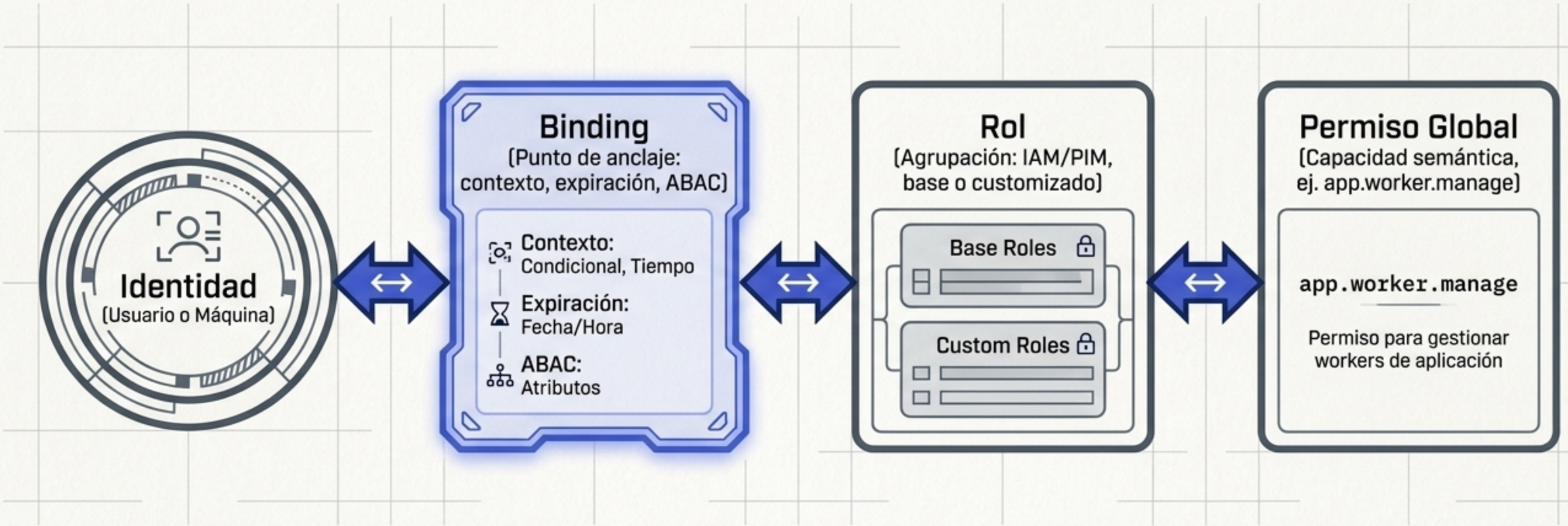
Single Source of Truth: Los permisos existen una única vez. Roles PIM e IAM instancian los mismos permisos semánticos sin duplicarlos.



Exclusions

El catálogo NO guarda estado: no contiene sesiones, bindings, tenants ni elevaciones activas. Solo definiciones reutilizables.

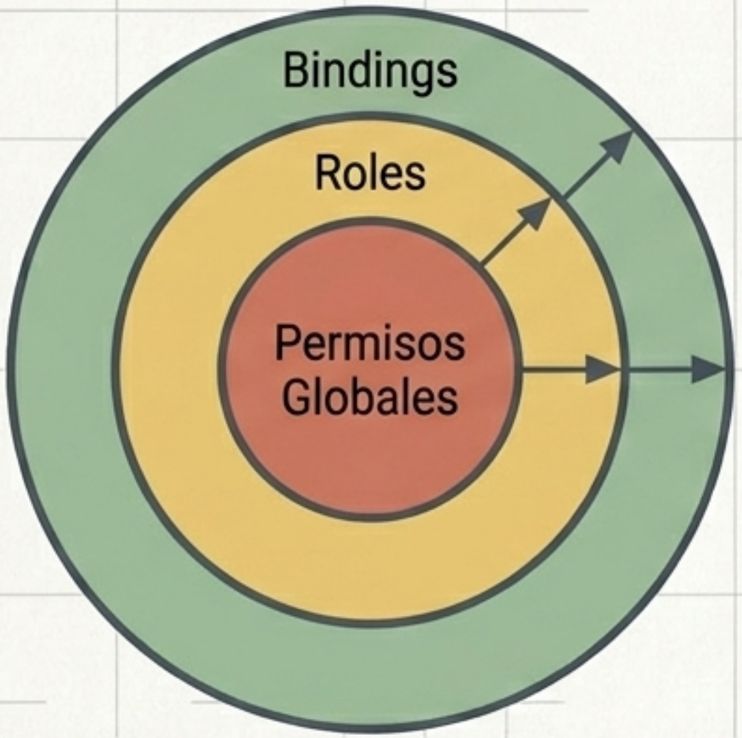
Anatomía de la Asignación: Bindings Autorizativos



Insight

El binding es la asignación efectiva. Relaciona dinámicamente identidades con agrupaciones de capacidades semánticas.

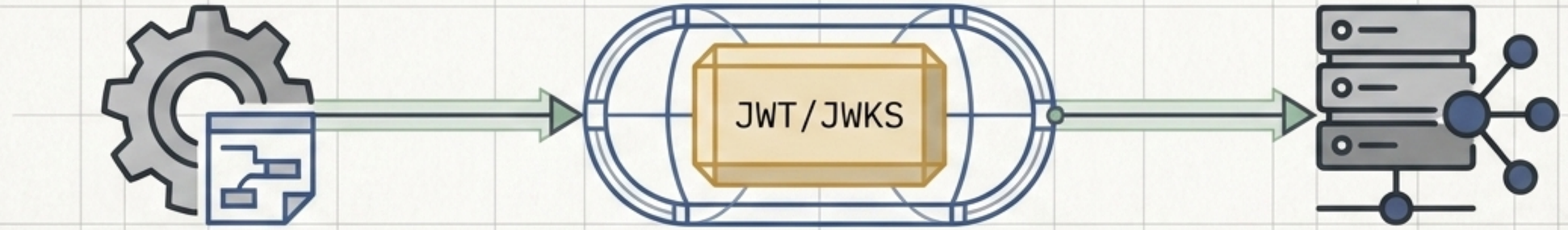
Control del “Blast Radius”: Estrategia ABAC Contextual



- **(Rojo) NUNCA sobre Permisos (Acceso):** Aplicar ABAC en permisos globales causa contaminación contextual, bloqueando operaciones del sistema al propagar restricciones a todos los roles que usan ese permiso.
- **(Verde) SÍ sobre Bindings y Roles**: La restricción contextual ABAC se aplica en las capas externas de asignación.

En el Plano de Acceso, los permisos permanecen como semántica autorizativa pura. La contextualización ocurre localmente en el Binding.

Gobernanza de Identidades Máquina y Service Principals



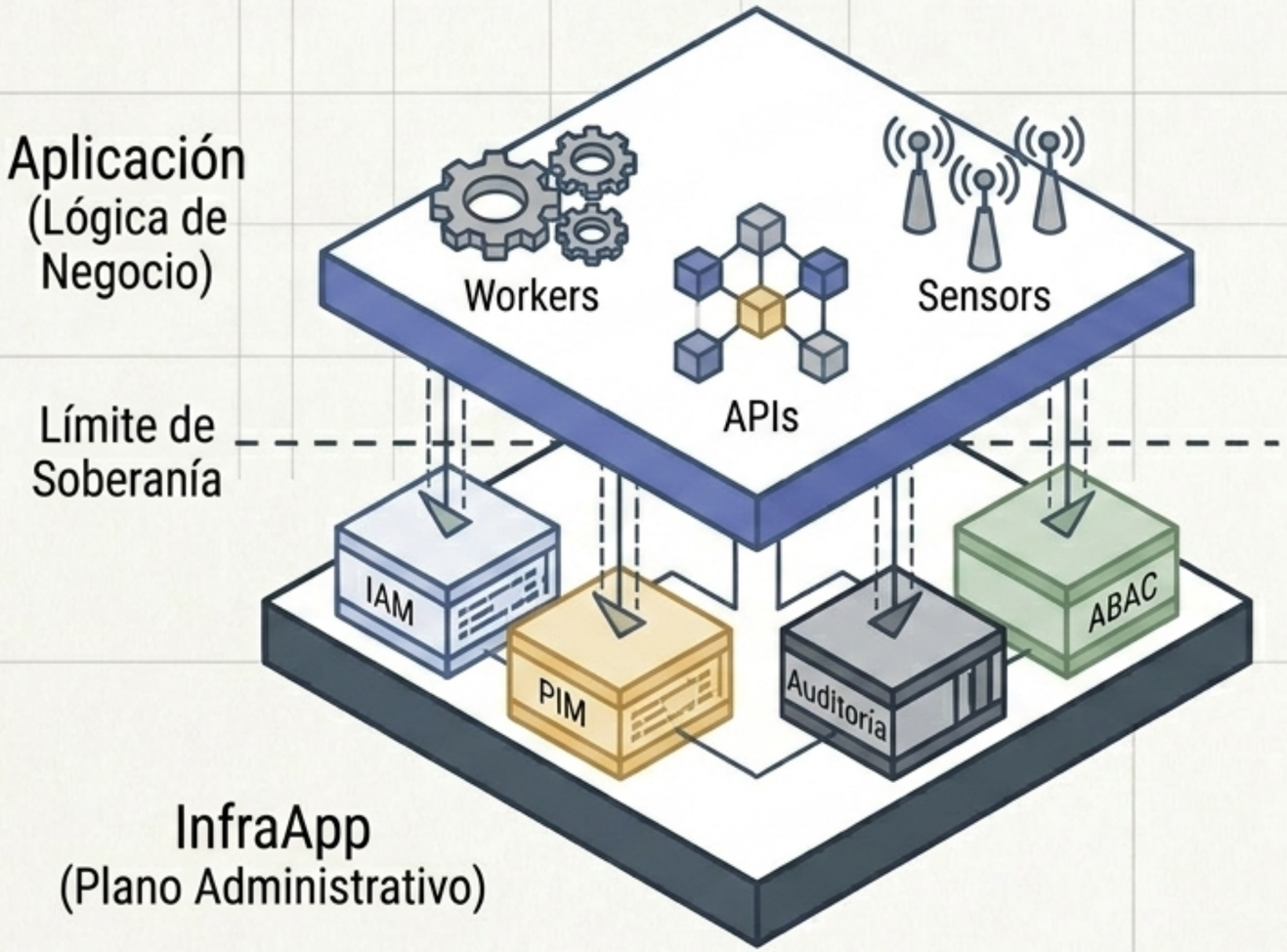
Sujetos No Humanos

Workers, procesos internos, pipelines, integración App ↔ App.

Mecanismo de Control

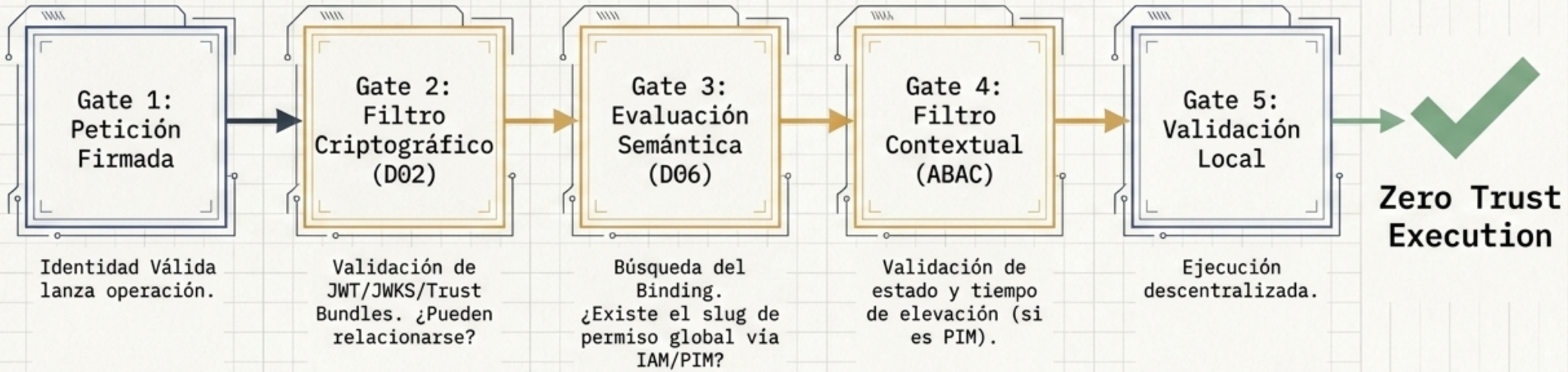
- Las identidades máquina operan principalmente bajo roles IAM persistentes.
- Están gobernadas por los mismos permisos globales, bindings y restricciones ABAC que las identidades humanas.
- La comunicación inter-aplicación exige workloads firmados criptográficamente (D02).

Integración de Aplicaciones: El Plano Administrativo Unificads



- **Autonomía Funcional:** La app **mantiene el 100% de control** sobre su lógica de negocio, APIs públicas y procesos internos.
- **Capa Administrativa Delegada:** La app sincroniza sus permisos (manifests) con InfraApp, consumiendo la plataforma para gobernar usuarios administrativos, elevación de privilegios y auditoría.

Flujo de Autorización Distribuida (Síntesis)



Conclusiones Arquitectónicas

SkyDefended InfraApp implementa una capa soberana de gobernanza autorizativa distribuida construida sobre confianza criptográfica explícita.

Control

Mantiene la autoridad semántica global.

Acceso

Materializa la Materialza la autorización operacional y contextual.

Aplicaciones

Consumen IAM/PIM/ABAC conservando absoluta autonomía funcional.

Architecture complete. End of D06 specification.