NEXOCYBER NETWORKS

NCN

Gobernanza Criptográfica Distribuida en SkyDefended InfraApp (D04)

Arquitectura de Lifecycle, Continuidad Trust y Mínima Exposición sobre Infraestructura Efímera

ESTADO: V1.2 CORE GOVERNANCE

TONO: ZERO TRUST ARCHITECTURE

AUTORIDAD: ISMAEL CRUZ CASASOLA

Qué NO es este sistema

- El objetivo NO es almacenar secretos.
- NO dependemos de variables de entorno.
- NO utilizamos secretos estáticos hardcodeados.
- NO emitimos tokens de infraestructura permanentes.
- NO basamos el trust puramente en el runtime.

Qué GOBIERNA realmente D04

- El objetivo es preservar la continuiidad trust bajo un runtime efímero y compromiso parcial.
- La autoridad criptográfica requiere gobernanza explícita.

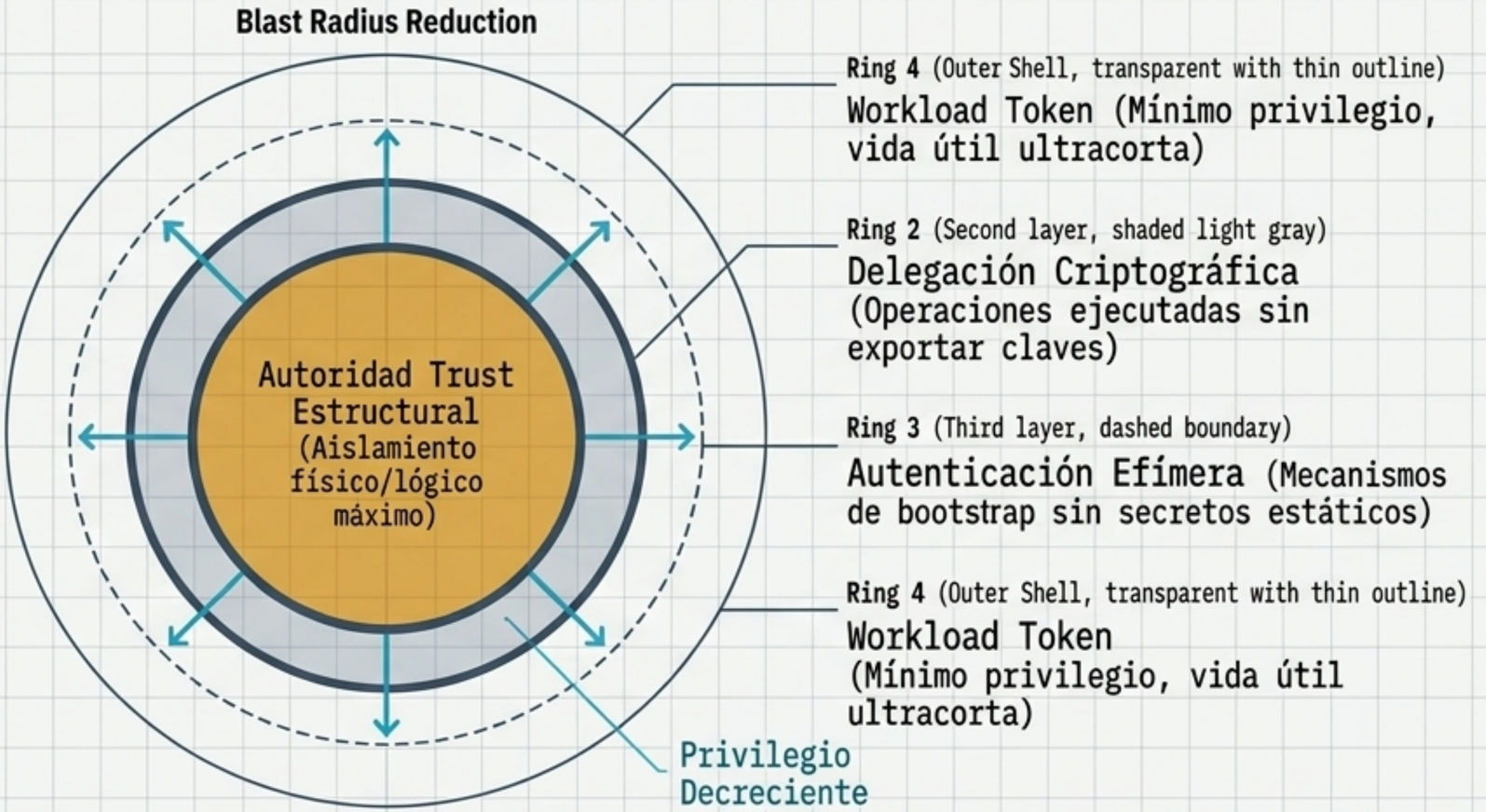
AXIOM_CORE

Runtime ≠ Identidad.
El workload es efímero; la identidad posee continuidad.
Custodia ≠ Confianza.

ARCHITECTURAL_GUIDELINE

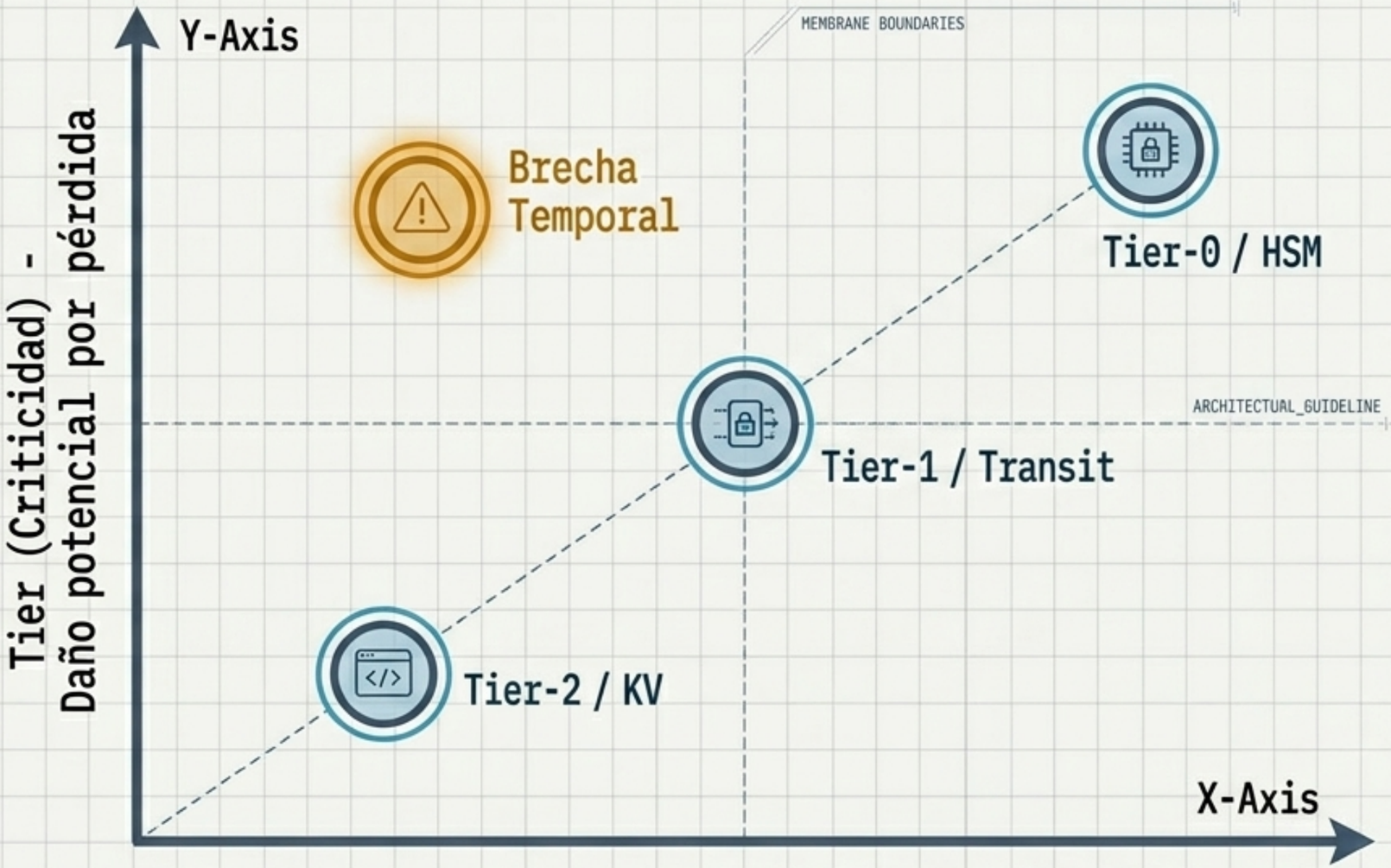
El Principio de Mínima Exposición

La arquitectura reduce progresivamente la exposición operacional de la autoridad criptográfica.



Métrica de éxito: Eliminación de privadas en runtime	Cero tokens permanentes	Contención de compromiso garantizada

Topología Ortogonal: Tier ≠ Nivel



La asignación temporal puede estar desalineada (Brecha Tier ↔ Nivel).

La arquitectura admite y audita esta coexistencia temporal mientras se prioriza la migración al Nivel objetivo.

Disección de la Criticidad Criptográfica

Tier-0 (Trust Root)	Tier-1 (Operational Critical)	Tier-2 (Operational Standard)

Definición:
Su compromiso rompe la confianza raíz del sistema.
 	
Política/Nivel:
HSM / Remote-sign. 100% no exportable. Auditoría y evidencía obligatoria.
 	
Ejemplos:
`SESSION_SIGNING_KEY`
`NCN_LICENSE_PRIVATE_KEY`
	Definición:
	Crítico pero recuperable mediante rotación. Blast radius contenido.
	
	Política/Nivel:
	Transit. No exportable cuando sea viable.
	
	Ejemplos:
	`INTERNAL_API_KEY`
	`STATE_SIGNING_KEY`
		Definición:
		Secretos operacionales que no forman parte de la autoridad trust estructural.
		Política/Nivel:
		KV. Rotación automatizable.
		
		Ejemplos:
		`DB credentials`
		`tokens SIEM`

El Lifecycle Criptográfico como Bucle de Control

Generación:
Asignación estricta de Owner, Tier y Nivel.

Custodia:
Almacenamiento aislado basado en Nivel.

Bootstrap:
Autenticación de carga de trabajo efímera.

Uso Operacional:
Delegado, minimizando exposición.

Rotación:
Programada, Emergencia o Estructural.

Revocación:
Bloqueo de trust e impedimento de reutilización.

Destrucción:
Eliminación real de persistencia y evidencia generada.

SCALE

Bootstrap Criptográfico Efímero

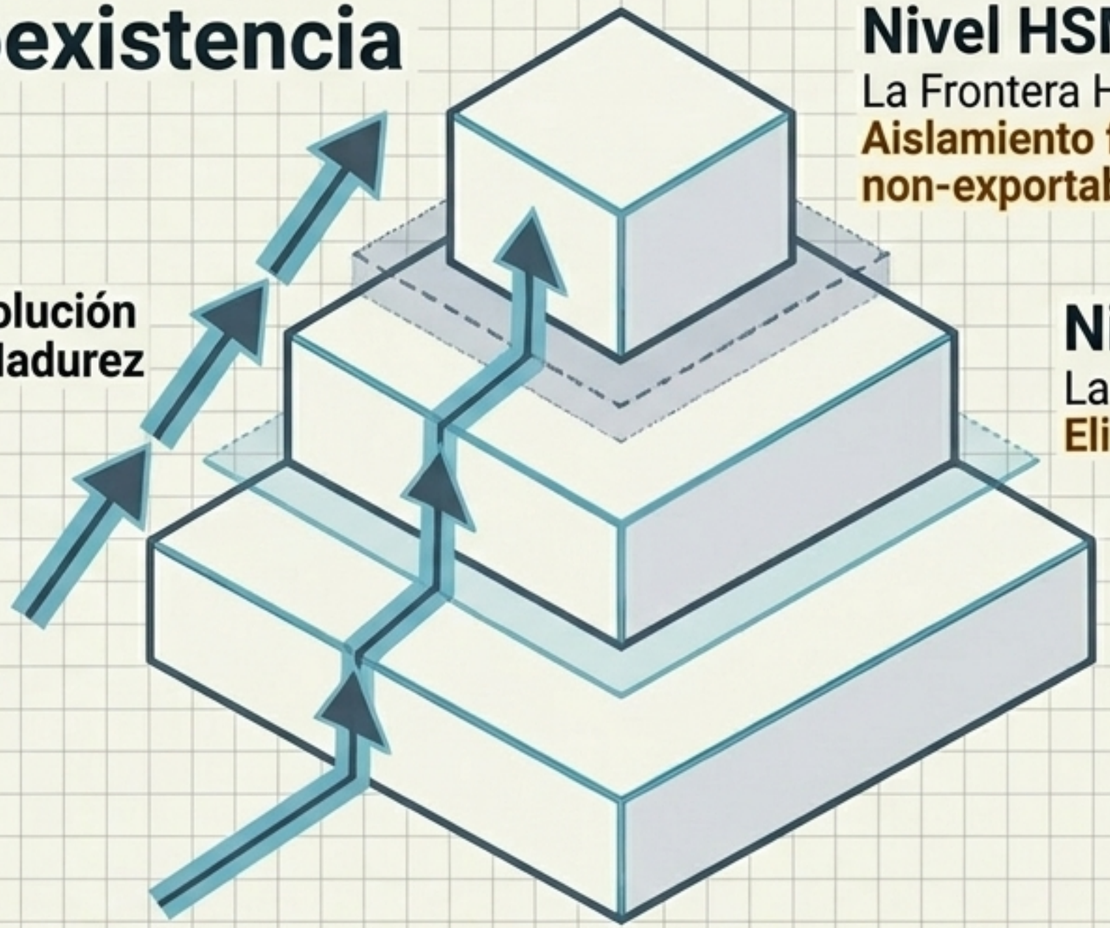
Transición segura de una Identidad Persistente a una Autorización de Workload efímera.

Mandatos de Arquitectura:

- Autenticación estrictamente efímera.
- Cero hardcoding de secretos.
- Recuperación controlada.

SCALE

Fronteras Operacionales: Evolución y Coexistencia



Nivel HSM

La Frontera Hardware.
Aislamiento físico máximo, non-exportable.

Nivel Transit

La Frontera Operacional.
Eliminación de privadas en runtime.

Nivel KV

Almacenamiento distribuido, latencia mínima, operaciones locales.

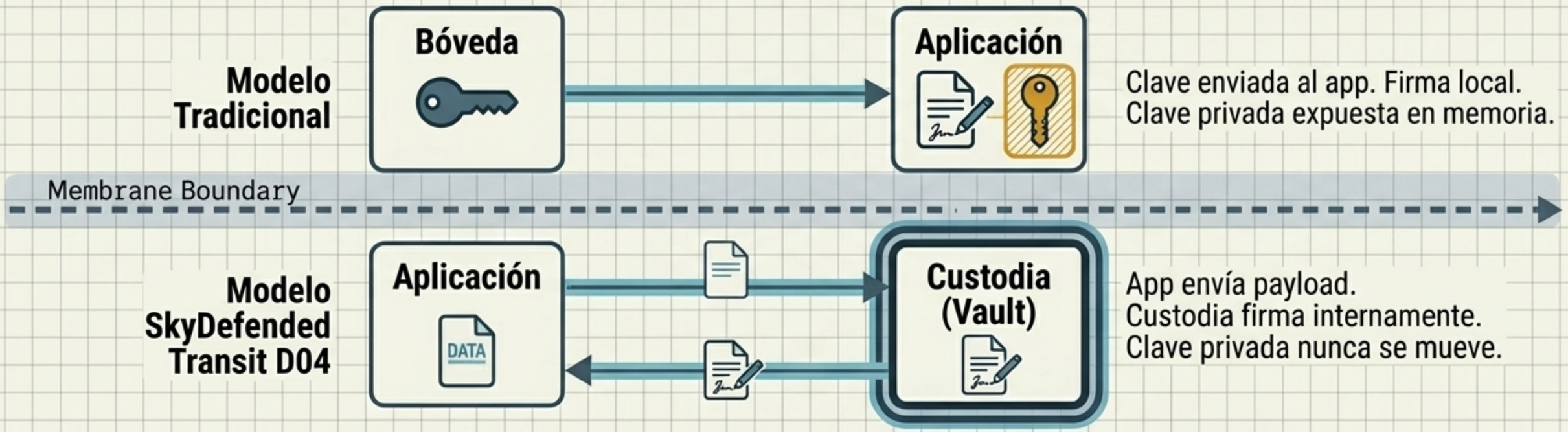
Principio de Coexistencia: SkyDefended InfraApp NO busca 'todo a HSM'. La arquitectura madura utiliza los tres niveles simultáneamente porque no todas las operaciones toleran la misma latencia o dependencia operacional.

SCALE

Deep-Dive: Transit como Frontera Operacional

Transit representa la eliminación progresiva de claves privadas dentro del runtime.

Comparativa de Hot-path Remoto



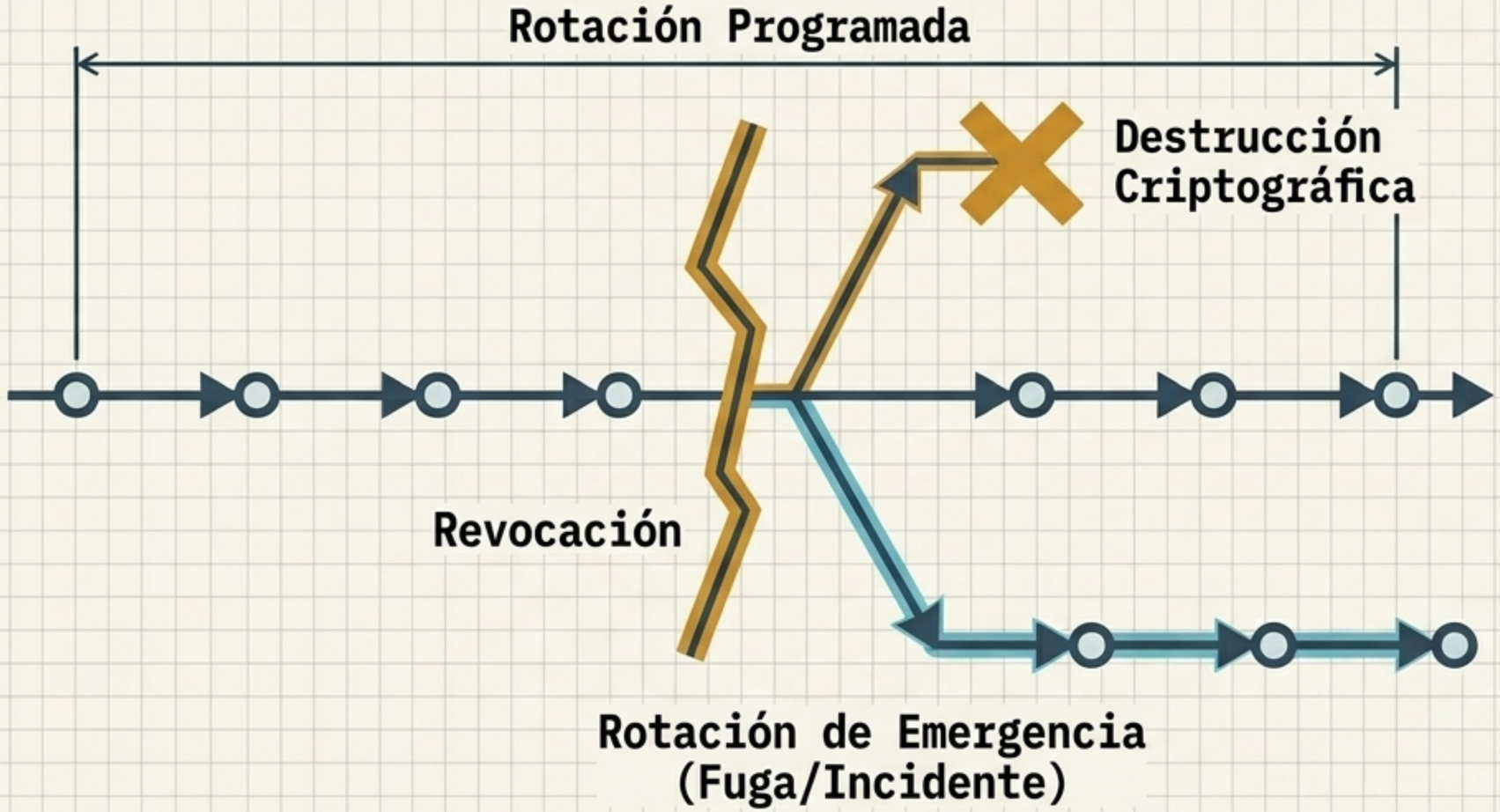
Axioma Definitivo: La clave privada JAMÁS abandona la bóveda lógica del sistema de custodia. El workload delega la firma, el cifrado y las operaciones sensibles.

SCALE

La Paradoja Arquitectónica: Resiliencia vs. Protección Máxima

El Conflicto	Decisión de Diseño
La máxima seguridad teórica aislada a menudo significa fracaso operacional. **La custodia NO puede romper la continuidad operacional de la infraestructura.**	- Mitigar la dependencia operacional del sistema de custodia. - Crítico para bootstrap, rotación y recovery. - NO debe ser una dependencia continua obligatoria para la validación distribuida. - La asignación Tier ↔ Nivel es una decisión de resiliencia.

Motores de Continuidad: Rotación y Revocación



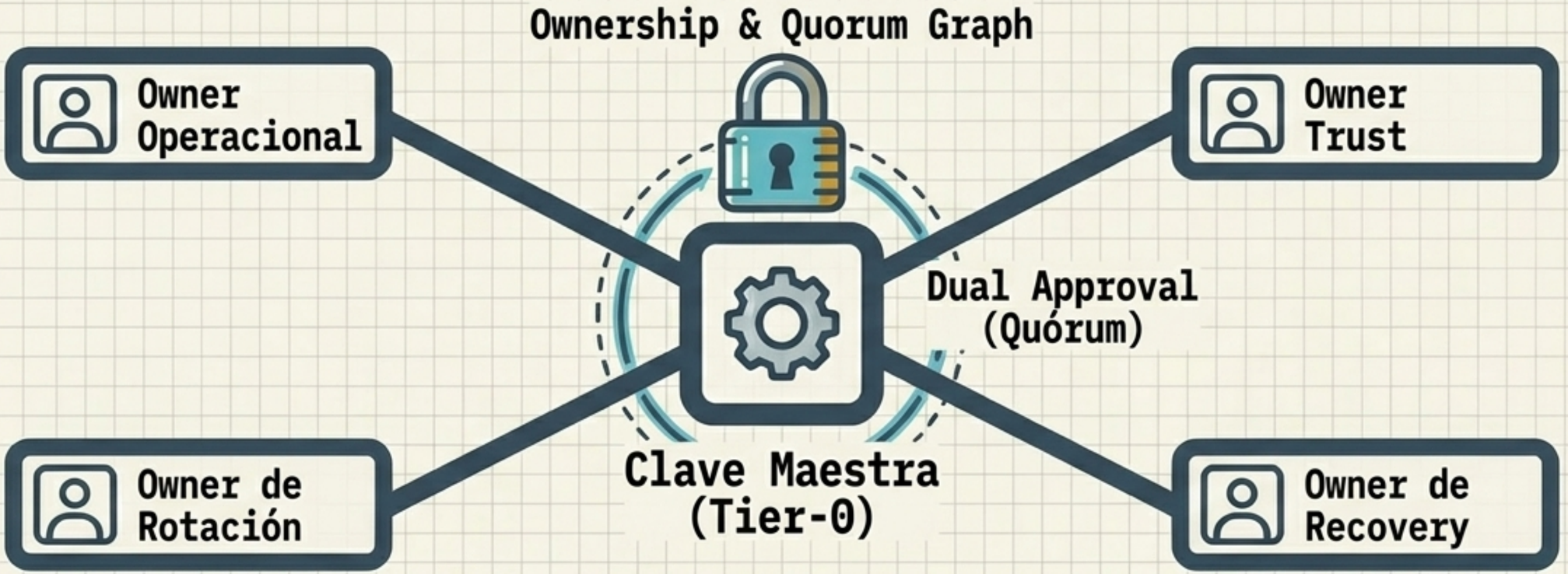
Tipos de Rotación:

1. **Programada:** Higiene periódica para reducir exposición.
2. **Emergencia:** Gatillada ante sospecha de compromiso.
3. **Estructural:** Migración de Tier/Nivel.

Regla de Destrucción:

Cortar la continuidad trust requiere eliminación real de la persistencia para impedir reutilización, dejando evidencia auditable.

Gobernanza Humana: Ownership Criptográfico y Quórum



Anchor Axiom	Quórum Operacional Tier-0
Una clave sin owner es una clave no gobernada.	- Aprobación Dual obligatoria para operaciones críticas. - Separación de funciones estricta. - Control multi-owner con evidencia explícita generada.

Evidencia, Auditoría y KPIs Criptográficos

Evidencia Obligatoria: Trazabilidad inmutable para toda generación, rotación, revocación, destrucción o migración de Tier/Nivel.

0

Brechas Detectadas:
Tier-0 fuera de HSM / Tier-1 fuera de Transit.

0

Orfandad:
Recuento de claves sin Owner asignado.

Higiene:
Claves expiradas o fuera de Tier objetivo rotadas.

Salud Operacional:
Rotaciones fallidas y Bootstrap failures en cero.

Stack Desplegado: SkyDefended InfraApp v1.2

Orquestación (Runtime efímero)

- Kubernetes Talos
- Cluster físico dedicado OVH

Custodia Criptográfica

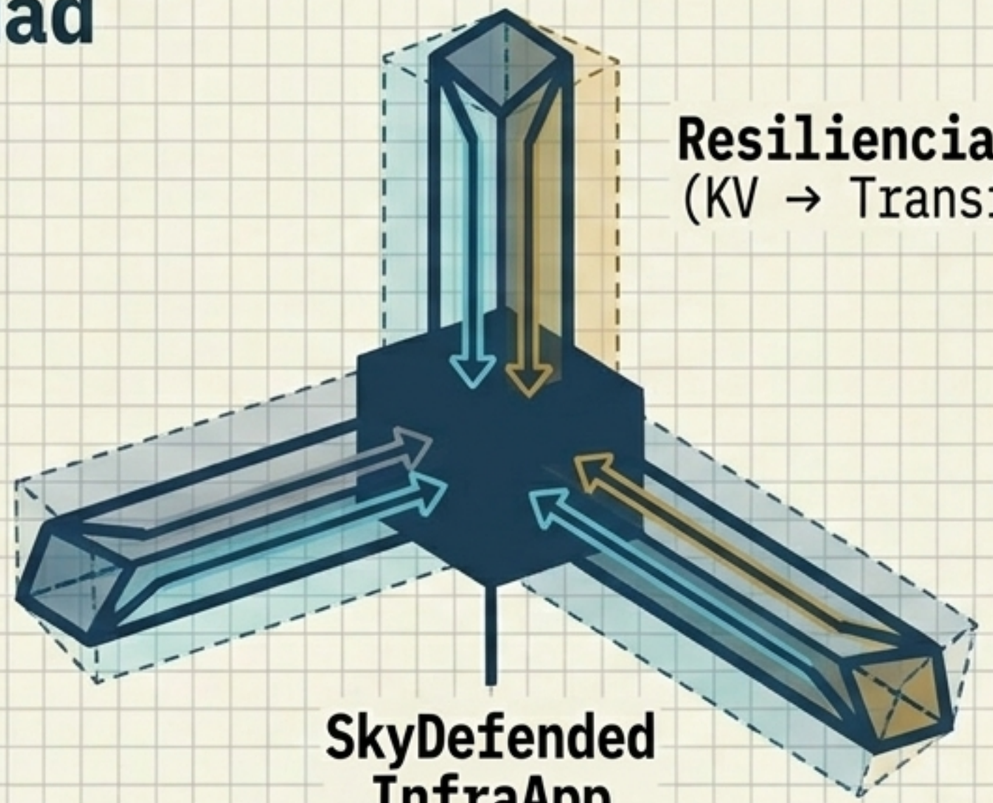
- HashiCorp Vault Raft (VM externa aislada)
- Kubernetes Auth v2.0

Estado actual:
Nivel KV generalizado,
Transit parcial,
HSM proyectado.

Integridad de Workload

- Cosign keyless & Sigstore
- Kyverno verify-image-signatures (Digest pinning)

Conclusión: La Arquitectura de la Continuidad



Resiliencia Operacional
(KV → Transit → HSM)

Continuidad Trust
(Identidad persistente)

SkyDefended InfraApp

Governance Profundo
(Reducción del blast radius)

**La plataforma no persigue la máxima protección teórica aislada.
Persigue el equilibrio arquitectónico perfecto entre la continuidad trust, la resiliencia operacional y un governance criptográfico distribuido.**