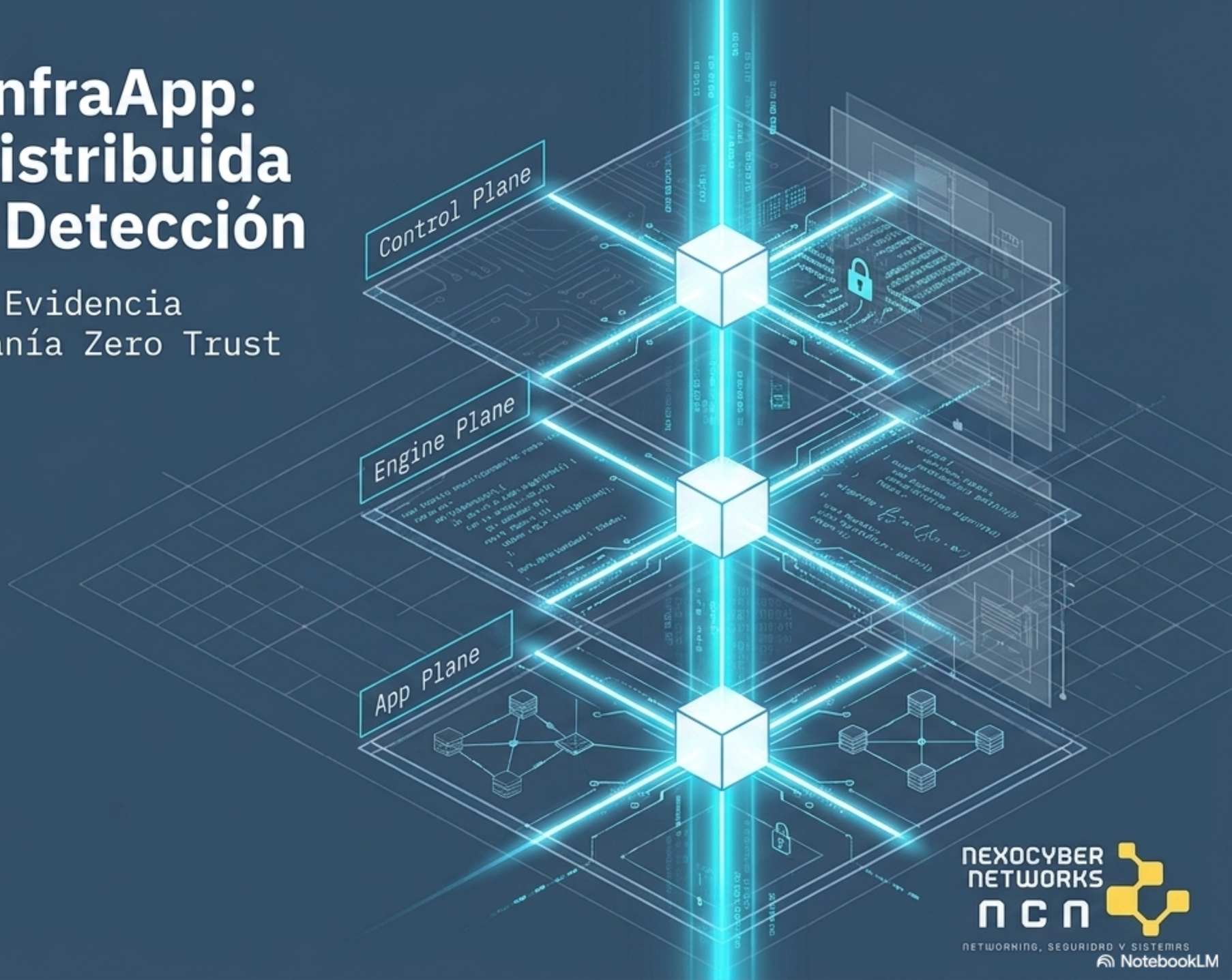
SkyDefended InfraApp: Arquitectura Distribuida de Evidencia y Detección

Topología Multi-Plano, Evidencia Tamper-Evident y Soberanía Zero Trust

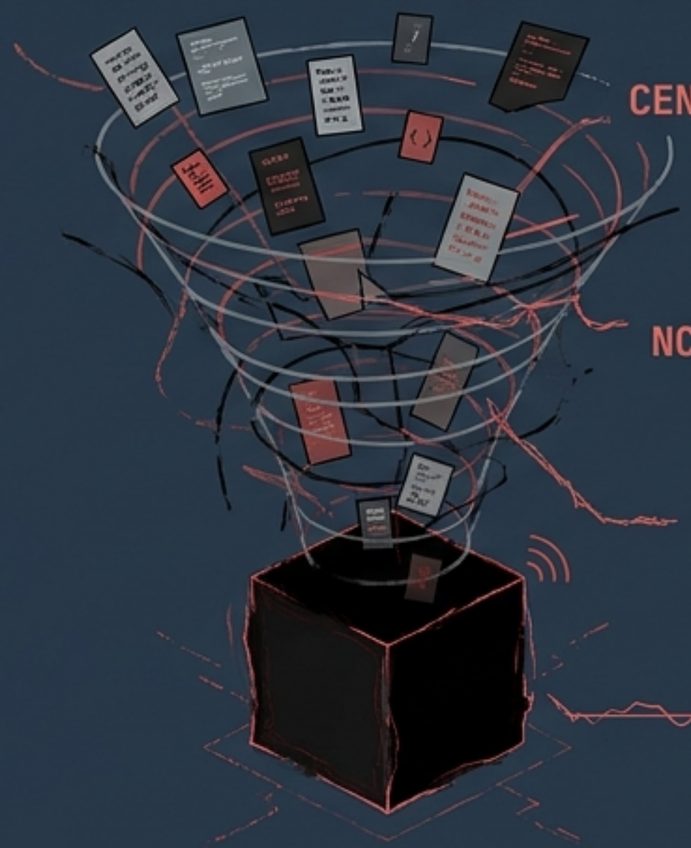


NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS

LA OBSERVABILIDAD NO CONSTITUYE UNA EXCEPCIÓN A ZERO TRUST

SkyDefended InfraApp abandona el anti-patrón de la observabilidad tradicional (centralización implícita) para implementar una arquitectura distribuida de soberanía operacional.

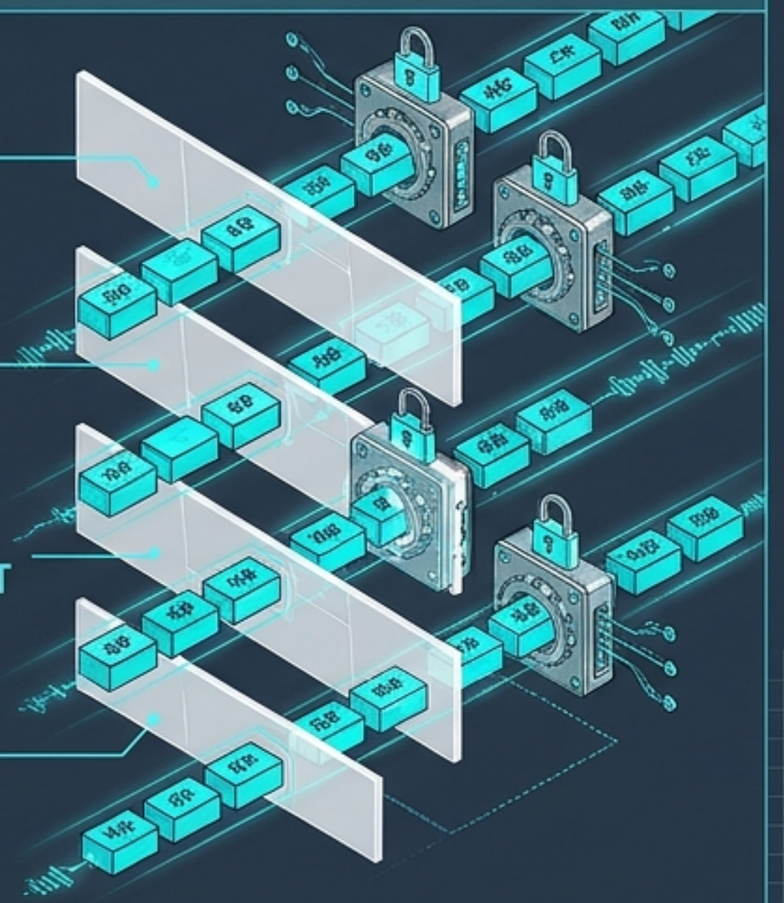
OBSERVABILIDAD TRADICIONAL



- CENTRALIZACIÓN CIEGA
- VISIBILIDAD NCN IMPLÍCITA
- MUTABILIDAD DE LOGS
- PROPIEDAD DILUIDA

EVIDENCIA SOBERANA SKYDEFENDED

- TOPOLOGÍA MULTI-PLANO
- VISIBILIDAD GOBERNADA POR CONSENT
- CADENA WORM TAMPER-EVIDENT
- SEPARACIÓN ESTRICTA DE PROPIEDAD

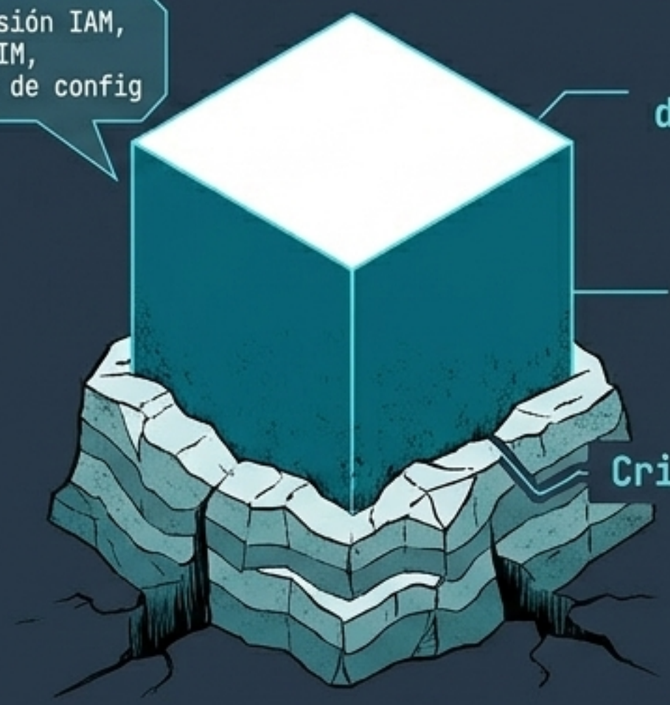


El Axioma Fundamental: Separación Estricta de Hechos y Juicios

La arquitectura garantiza su valor probatorio dividiendo el dominio analítico en dos capas inmiscibles.

Audit (Hechos)

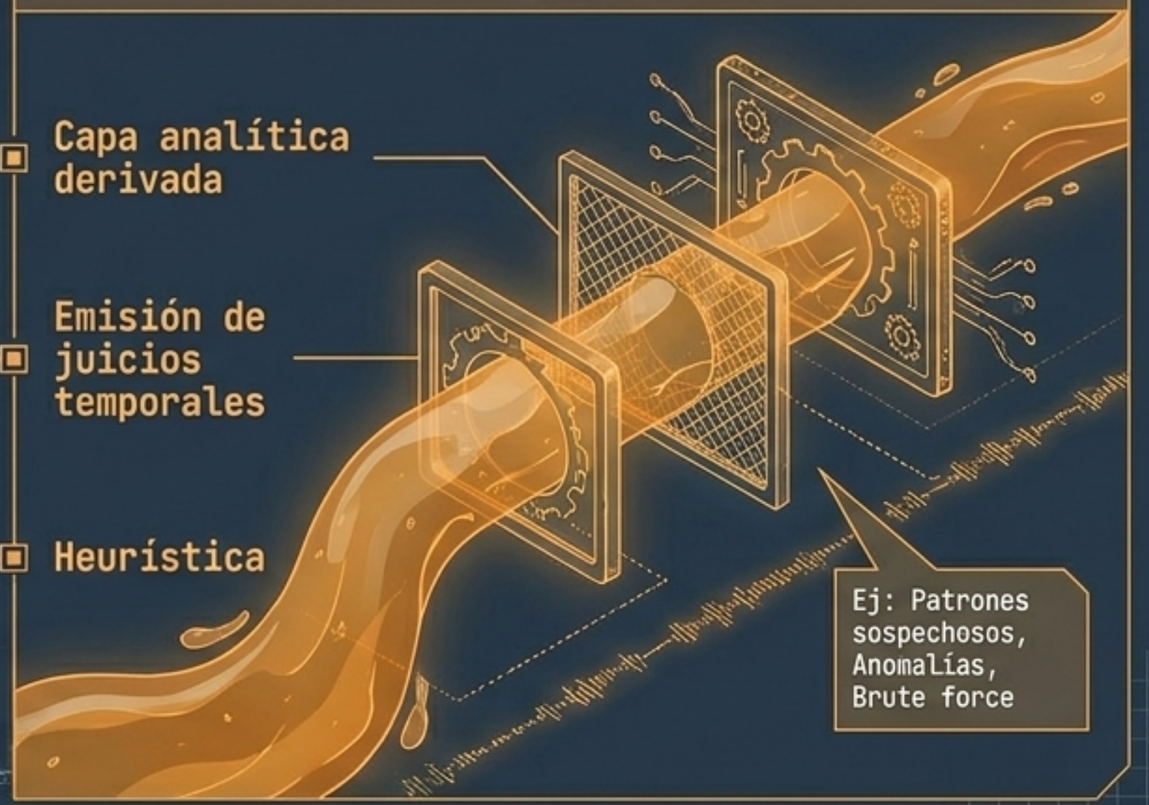
Ej: Decisión IAM, Acceso PIM, Mutación de config



- Registro determinista
- Fuente probatoria primaria
- Cripto-anclado (WORM)

Guard (Juicios)

- Capa analítica derivada
- Emisión de juicios temporales
- Heurística



Ej: Patrones sospechosos, Anomalías, Brute force

Audit es la evidencia legal; Guard es la capa operativa.

Topología de Planos y Dominios de Confianza

Ningún dominio operacional recibe acceso implícito a evidencia perteneciente a otro dominio. El aislamiento es topológico.

Matriz de Soberanía: Carriles de Propiedad (A-E)

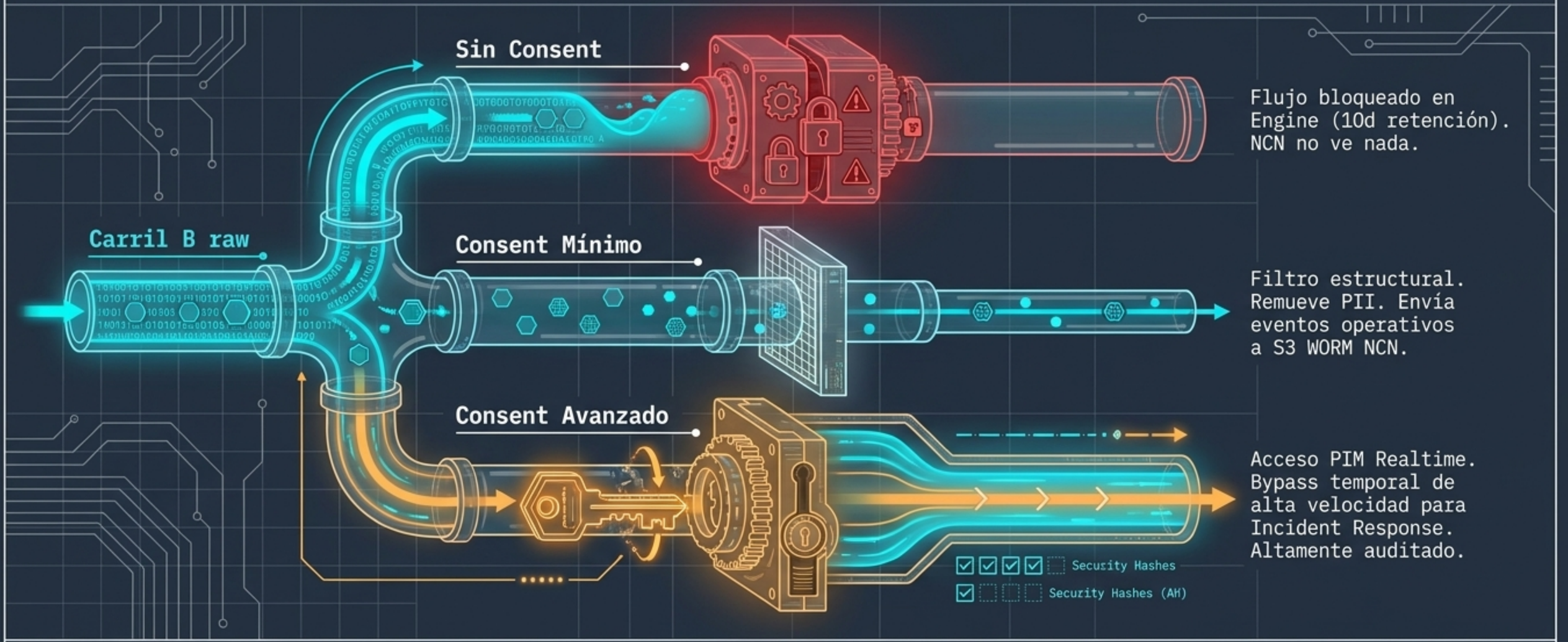
El ciclo de vida y la visibilidad de la evidencia están dictados de forma determinista por su carril de origen.

Heatmap Matrix

Carril	Dueño Lógico	Persistencia Hot	Cold WORM	Visibilidad Default
Carril A (Control/NCN)	NCN	60d	5y S3 NCN	NCN
Carril B (Tenant Raw)	Tenant	10d Engine	SIEM Tenant	Tenant (Isolado)
Carril C (Engine Infra)	NCN	60d	5y S3 NCN	NCN Platform
Carril D (Operator)	NCN	60d	5y S3 NCN	NCN
Carril E (App Infra)	NCN	60d	5y S3 NCN	NCN Platform

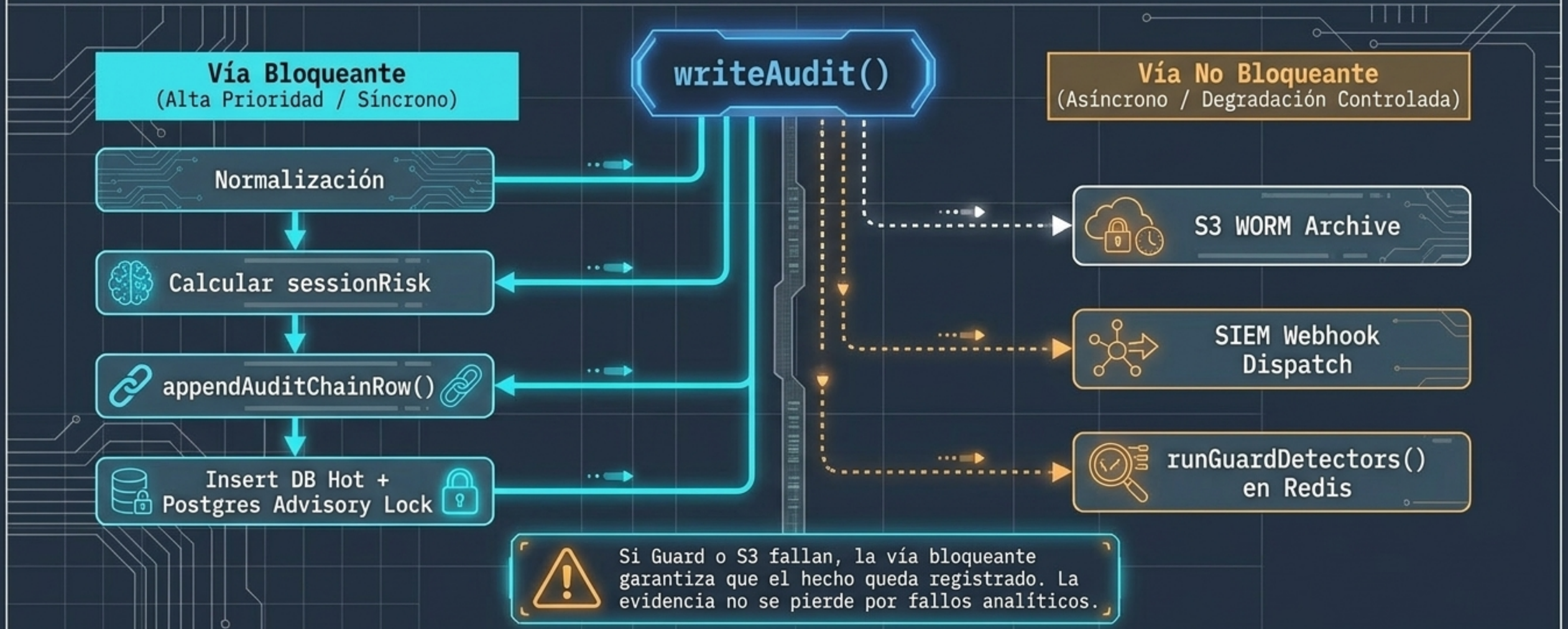
Gobernanza del Dato: El Mecanismo de Consentimiento (Tenant Consent)

La visibilidad sobre el Carril B raw es opaca por defecto. El flujo hacia el dominio NCN está físicamente bloqueado hasta que se activan las esclusas criptográficas.



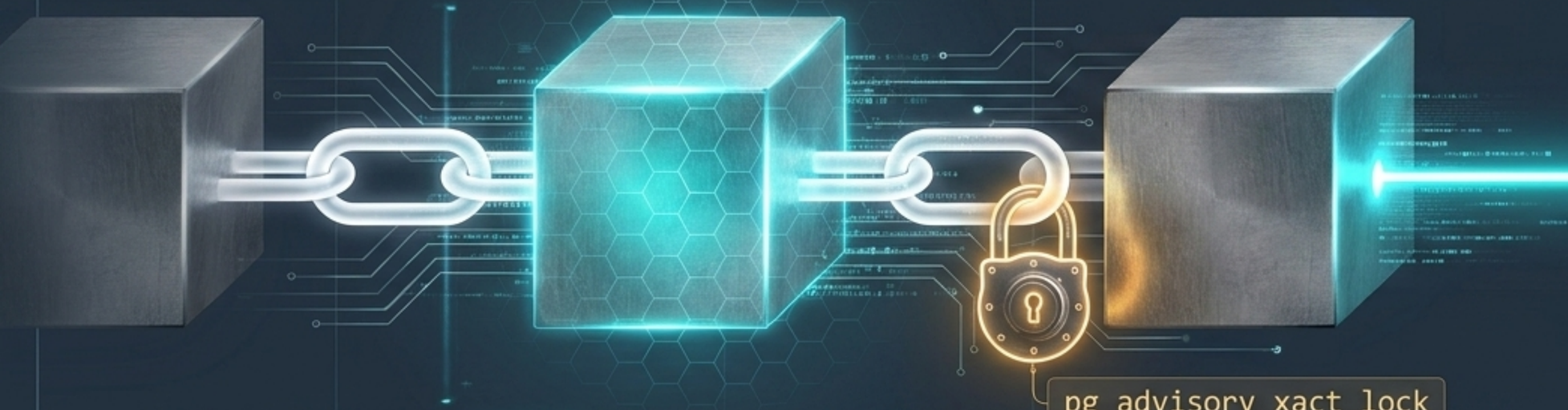
Ingestión Resiliente: Pipeline Runtime de writeAudit()

La entrada canónica está diseñada para garantizar registro probatorio inmediato mientras aísla analíticas asíncronas para prevenir caídas en cascada.



Integridad Forense: Cadena Hash Tamper-Evident

Las bifurcaciones concurrentes y alteraciones retrospectivas son imposibles matemáticamente mediante anclaje de hash iterativo y bloqueos transaccionales.



`rowHash = SHA256(prevHash || canonicalSerialize (row_actual))`

`pg_advisory_xact_lock`

Previene lecturas simultáneas del mismo prevHash

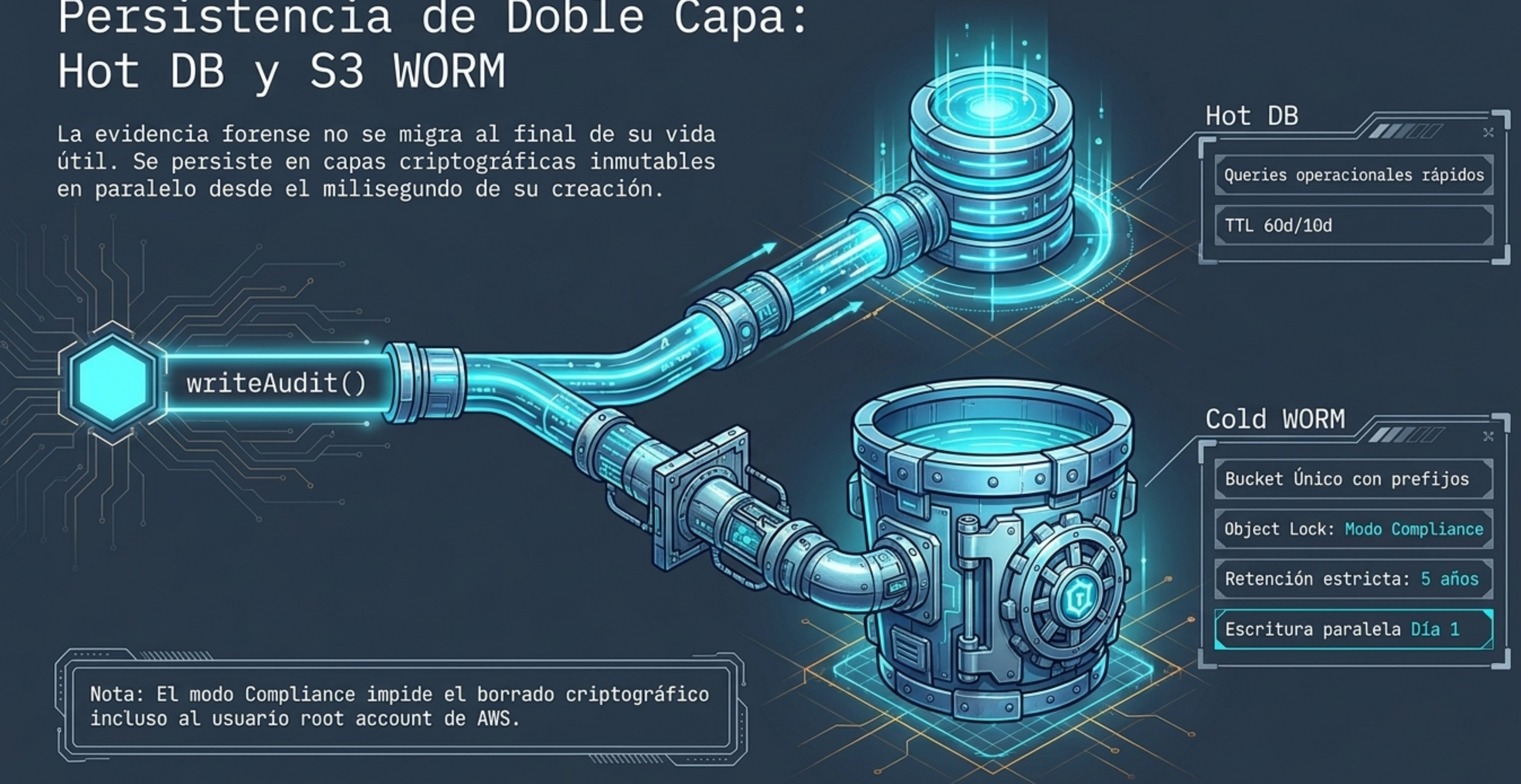
`Anchoring Endpoint: /v1/audit/chain/head`

`Anchoring Endpoint: /v1/audit/chain/head`

Proyección externa a SIEM para anclaje de tiempo.

Persistencia de Doble Capa: Hot DB y S3 WORM

La evidencia forense no se migra al final de su vida útil. Se persiste en capas criptográficas inmutables en paralelo desde el milisegundo de su creación.



Hot DB

- Queries operacionales rápidos
- TTL 60d/10d

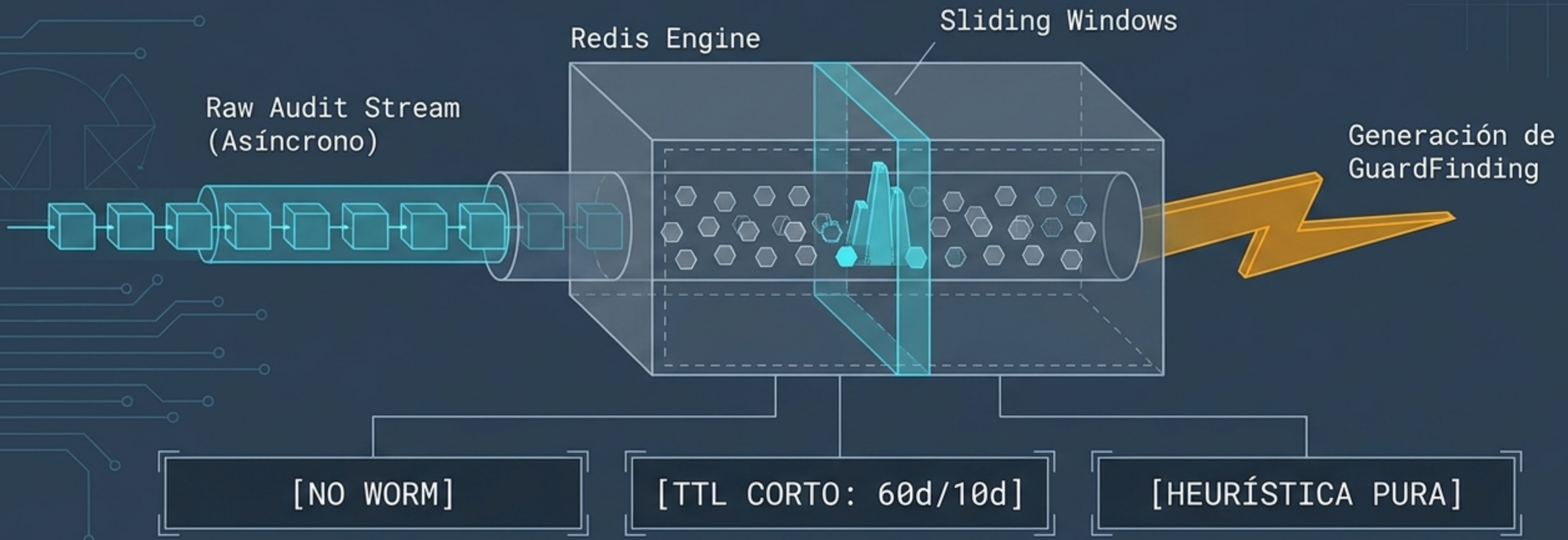
Cold WORM

- Bucket Único con prefijos
- Object Lock: Modo Compliance
- Retención estricta: 5 años
- Escritura paralela Día 1

Nota: El modo Compliance impide el borrado criptográfico incluso al usuario root account de AWS.

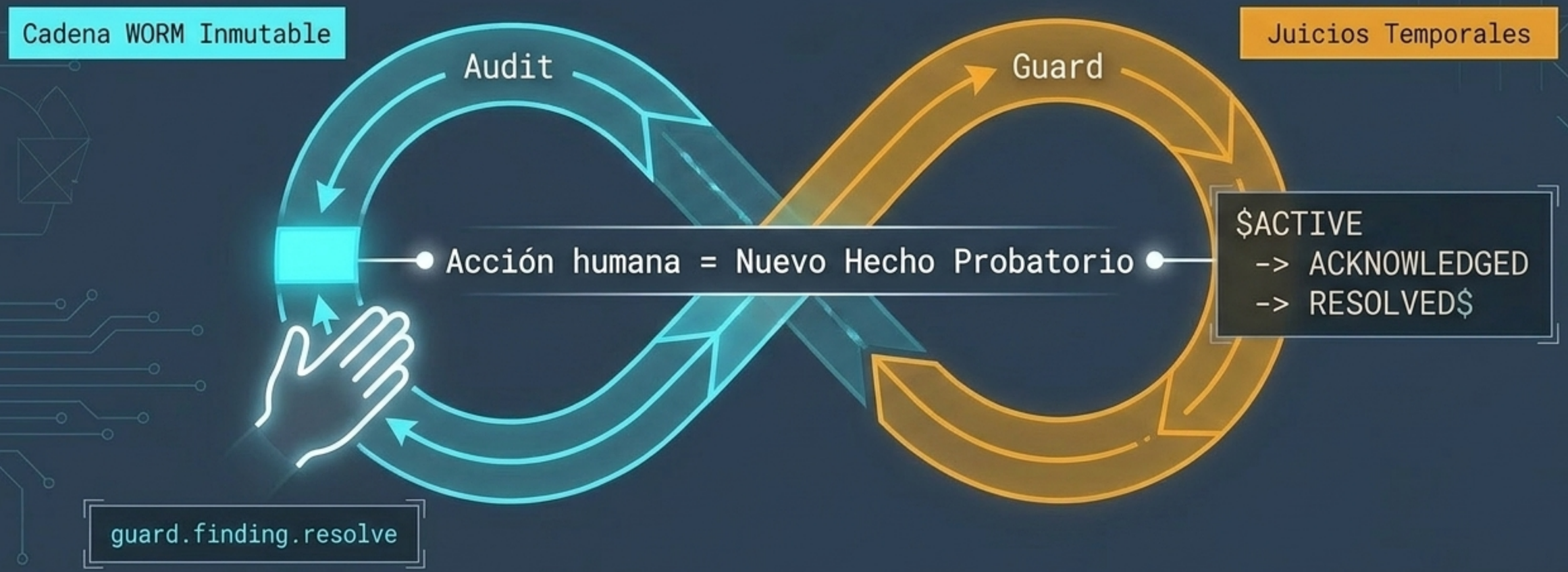
Guard: La Capa Derivada y Detección Contextual

Guard intercepta asíncronamente el stream de eventos Audit para aplicar heurística y memoria de estado temporal sin alterar la cadena probatoria.



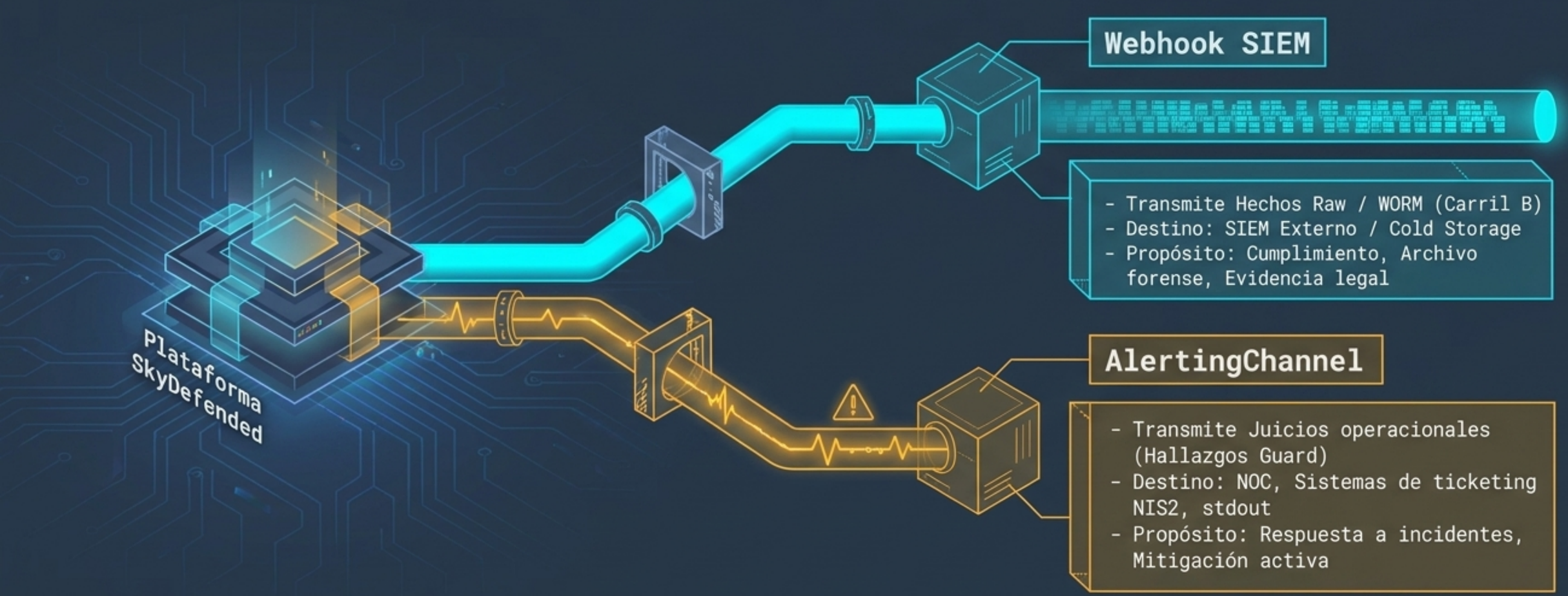
Simbiosis Audit-Guard: Ciclo de Vida del Hallazgo

La asimetría del diseño es intencional: Guard genera juicios efímeros, pero las decisiones humanas sobre esos juicios se inyectan de vuelta como evidencia inmutable.



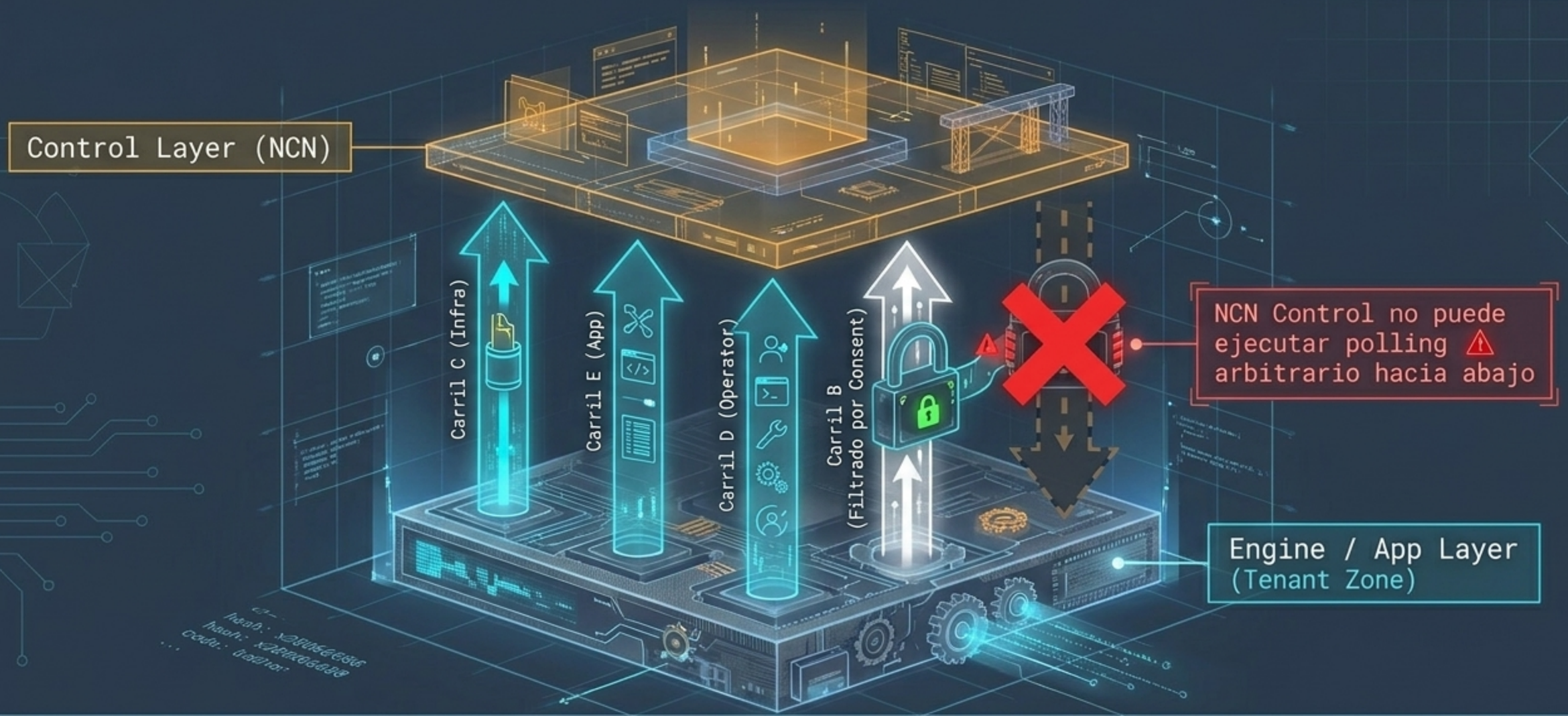
Enrutamiento Saliente: SIEM Webhook vs AlertingChannel

El destino de los datos depende de su naturaleza fundamental. Se mantienen rutas de salida paralelas para no contaminar sistemas operativos con raw data masivo, ni vaciar SOCs sin contexto.



Push Upward Asimétrico: Engine → Control

Para preservar el santuario Zero Trust, la arquitectura permite visibilidad centralizada mediante un flujo estrictamente unidireccional. Control nunca extrae; Engine siempre empuja.



Interrogación Distribuida y Replay Forense

La telemetría descentralizada requiere un modelo de consulta adaptable a la severidad del incidente y la temperatura del dato.

Hot Query

UI estándar, indexación ultra-rápida. Cobertura de incidentes recientes (10d-60d).

Advanced Realtime (PIM)

Tailing de raw data en vivo. Requiere desbloqueo físico con llave PIM. Trazabilidad de auditoria extrema.

Operator Console

S3 Forensic Query

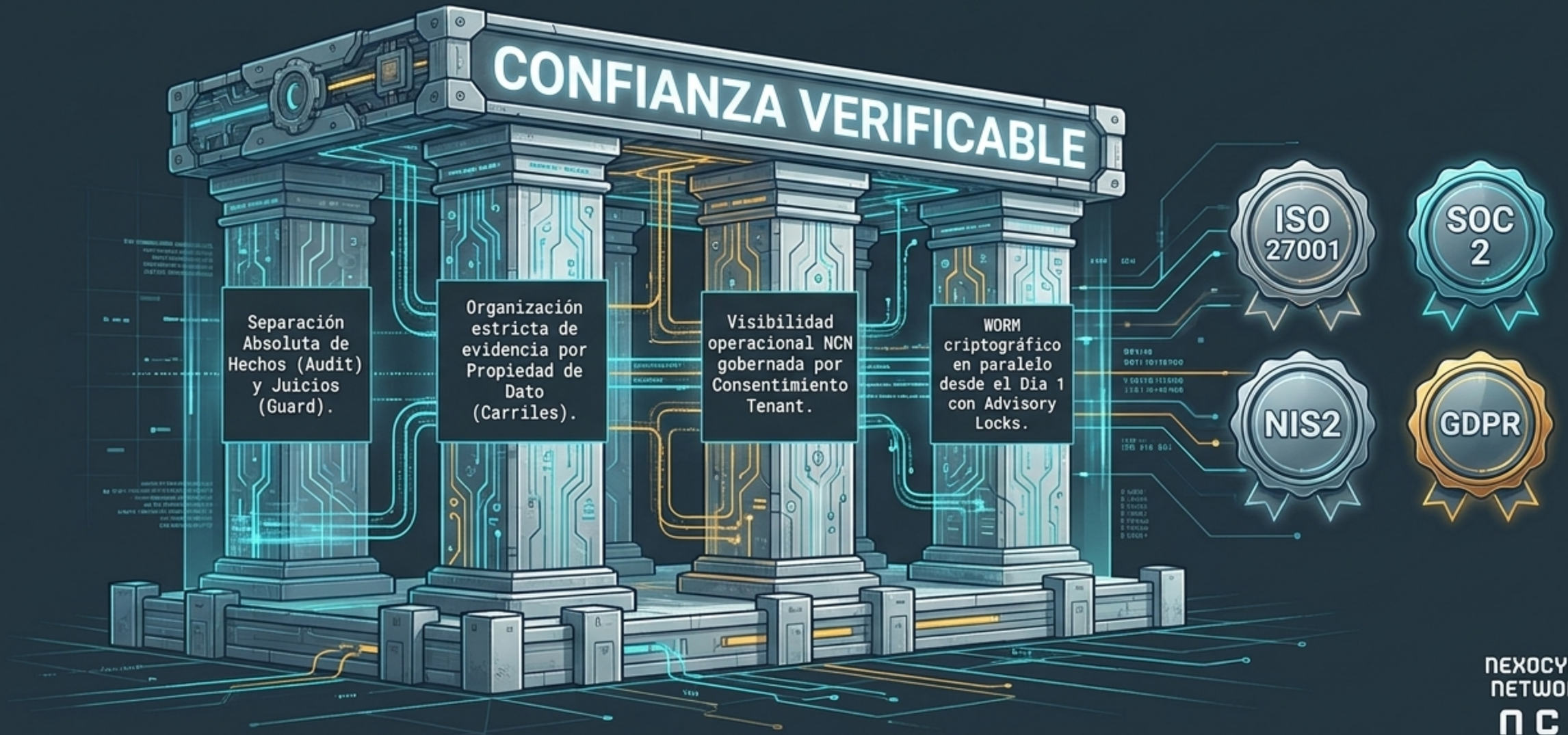
Consulta en frío contra almacenamiento compliance de 5 años. Reconstrucción histórica legal.

Replay Forense

Extracción de eventos WORM cold y reinyección retrospectiva en nuevos detectores Guard para evaluar firmas perdidas.

Conclusión Arquitectónica: Invariantes para la Confianza Verificable

SkyDefended InfraApp transforma el logging tradicional en una cadena forense soberana e inquebrantable. Mientras se respeten las invariantes, la plataforma garantiza cumplimiento automático.



NEXOCYBER NETWORKS

NCN

NETWORKING, S

NotebookLM