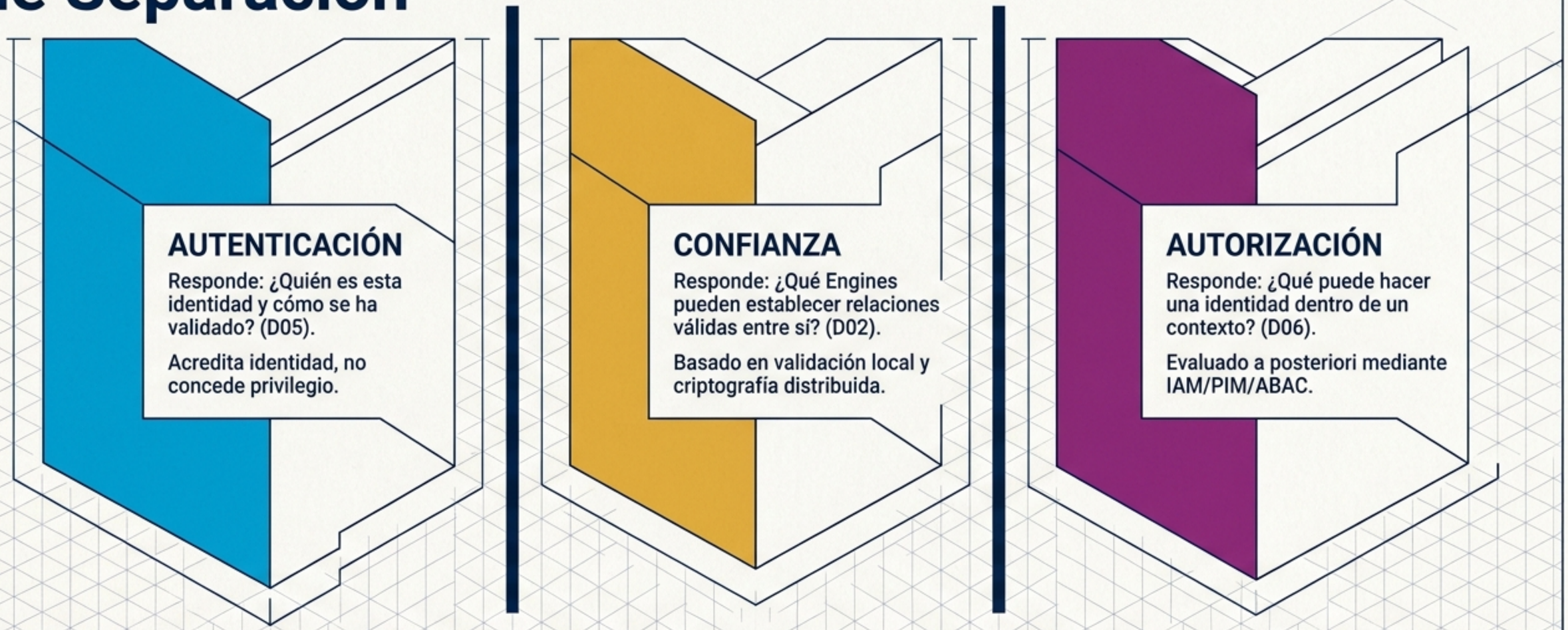
NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS

Modelo de Autenticación y Federación Distribuida

Arquitectura Zero Trust Multi-Plano (D05)

Documento arquitectónico canónico para SkyDefended InfraApp v1.0.

El Principio Fundamental de Separación



AUTENTICACIÓN

Responde: ¿Quién es esta identidad y cómo se ha validado? (D05).

Acredita identidad, no concede privilegio.

CONFIANZA

Responde: ¿Qué Engines pueden establecer relaciones válidas entre sí? (D02).

Basado en validación local y criptografía distribuida.

AUTORIZACIÓN

Responde: ¿Qué puede hacer una identidad dentro de un contexto? (D06).

Evaluado a posteriori mediante IAM/PIM/ABAC.

Ninguna identidad obtiene privilegio por el simple hecho de autenticarse.

DNA Zero Trust de la Plataforma

Fundamentos Aprobados

- ✓ NIST SP 800-207 (Zero Trust Architecture)
- ✓ Identity-Centric Security & Explicit Verification
- ✓ Just-In-Time (JIT) Privilege Elevation
- ✓ Decentralized Validation

No basamos autenticación en:

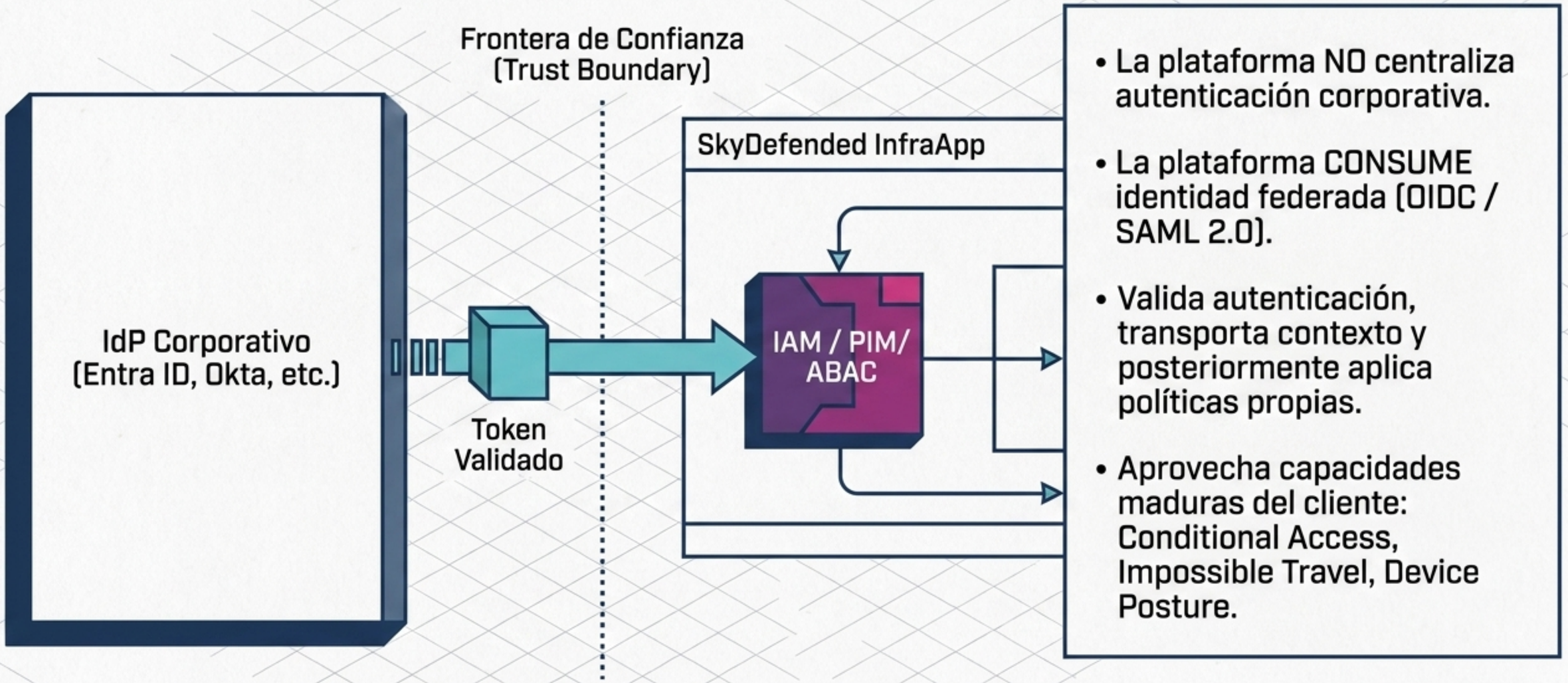
- ✗ Redes privadas o proximidad topológica
- ✗ Pertenencia a un cluster o IPs
- ✗ Infraestructura compartida o localización física

Alineado con NIST SP 800-63-3 (Digital Identity) e ISO/IEC 27001:2022.

Fronteras de Dominios de Autenticación

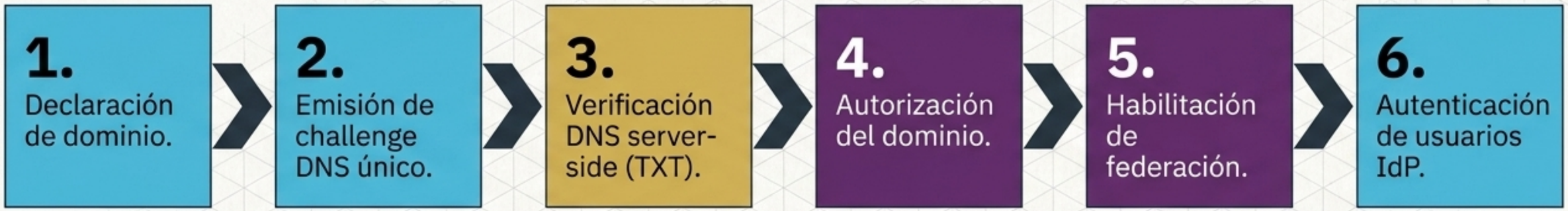
	PLANO DE CONTROL	PLANO DE ACCESO
Propósito	Gobierno de la estructura raíz y lifecycle administrativo global.	Dominio operacional soberano del tenant.
Propietario / Autoridad	SkyDefended InfraApp (NCN).	El Tenant (Cliente).
Identidad Diaria	Federación corporativa NCN (Entra ID).	Federación corporativa del cliente (OIDC/SAML).
Usuarios Locales	5 Owners locales soberanos.	5 Owners locales del tenant.
Regla de Aislamiento	NO participa en la operación funcional del tenant.	NO tiene visibilidad sobre la estructura raíz.

Soberanía del Tenant: InfraApp NO es el IdP



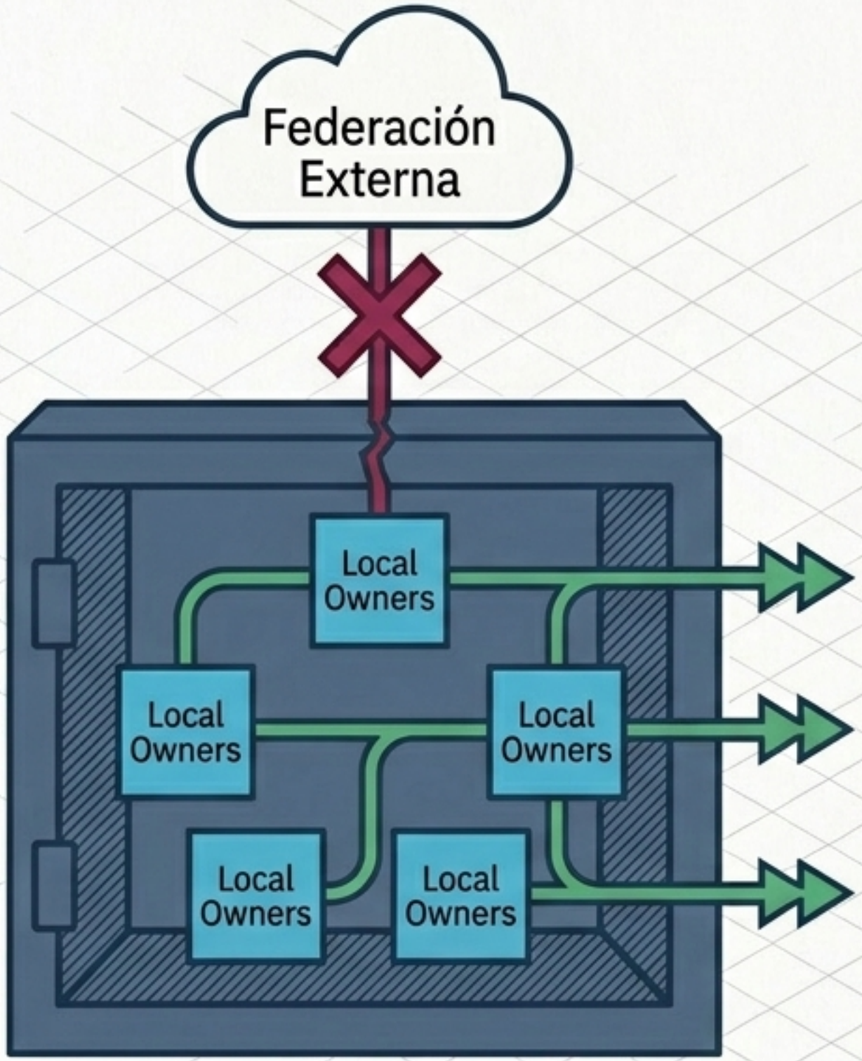
- La plataforma NO centraliza autenticación corporativa.
- La plataforma CONSUME identidad federada (OIDC / SAML 2.0).
- Valida autenticación, transporta contexto y posteriormente aplica políticas propias.
- Aprovecha capacidades maduras del cliente: Conditional Access, Impossible Travel, Device Posture.

Validación Estricta de Dominios Federados



La confianza no se basa en ‘un **login Microsoft**’.
Exige validación explícita para evitar suplantación.

Owners Locales y Resiliencia Soberana



Propósito: Continuidad operacional, recuperación ante pérdida de federación (Break-glass), y bootstrap soberano.

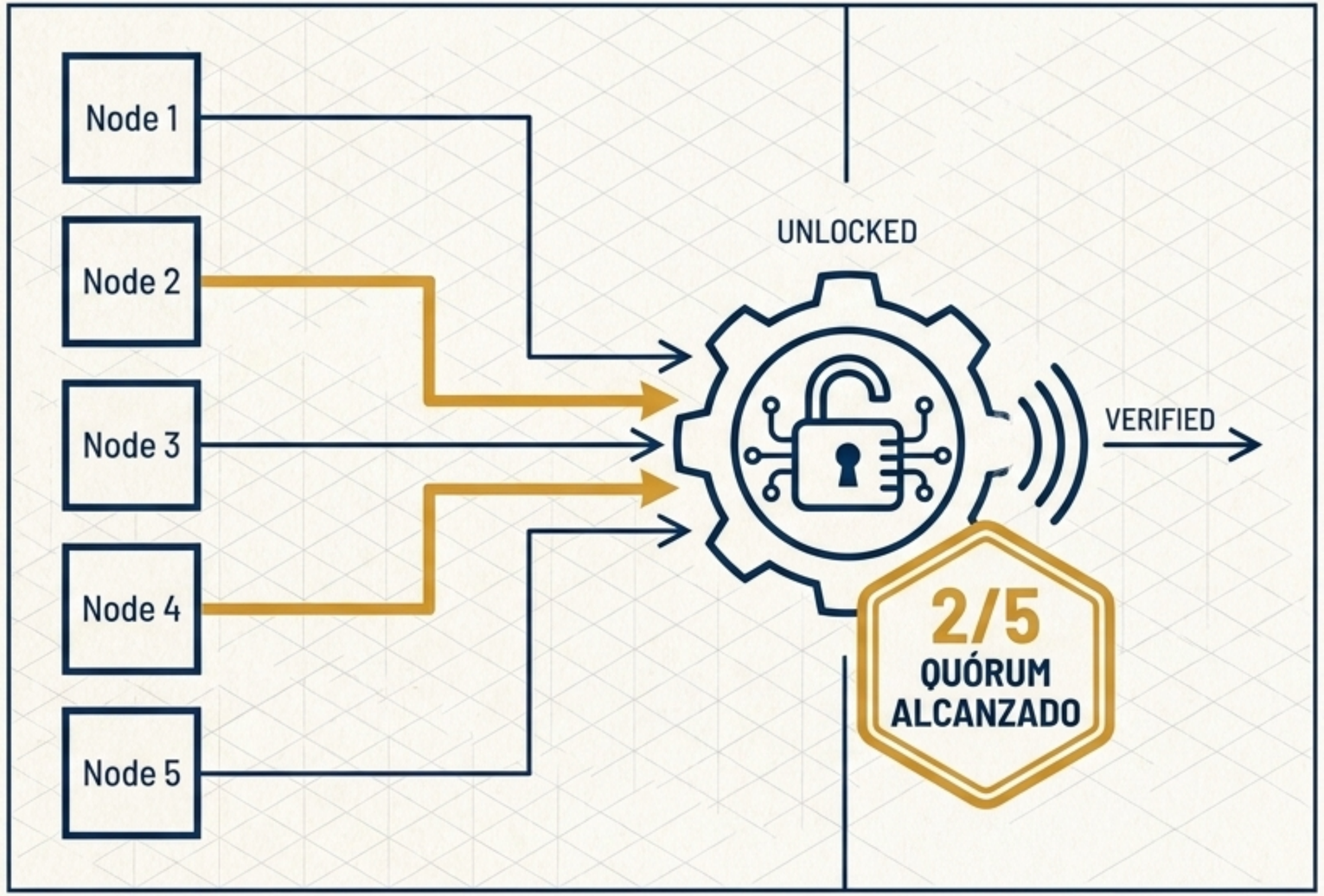
Diseño: 5 administradores owner por tenant (y 5 en el Plano de Control).

Independencia: Utilizan cualquier dominio, requieren unicidad de email, NO dependen de federación corporativa. No pensados para operación diaria.

Custodia Criptográfica y Step-Up Authentication

Custodia	Step-Up
Custodia: TOTP (RFC 6238). SMS explícitamente excluido (NIST AAL2). Semilla nunca en plaintext. **Cifrado:** Vault Transit, AES-256-GCM, custodia non-exportable.	**Step-Up:** Operaciones destructivas requieren MFA reciente (ventana máxima: 5 minutos). **Grace Period:** Configurable (0-5 días) para balancear onboarding y seguridad obligatoria.

Quórum Administrativo Distribuido



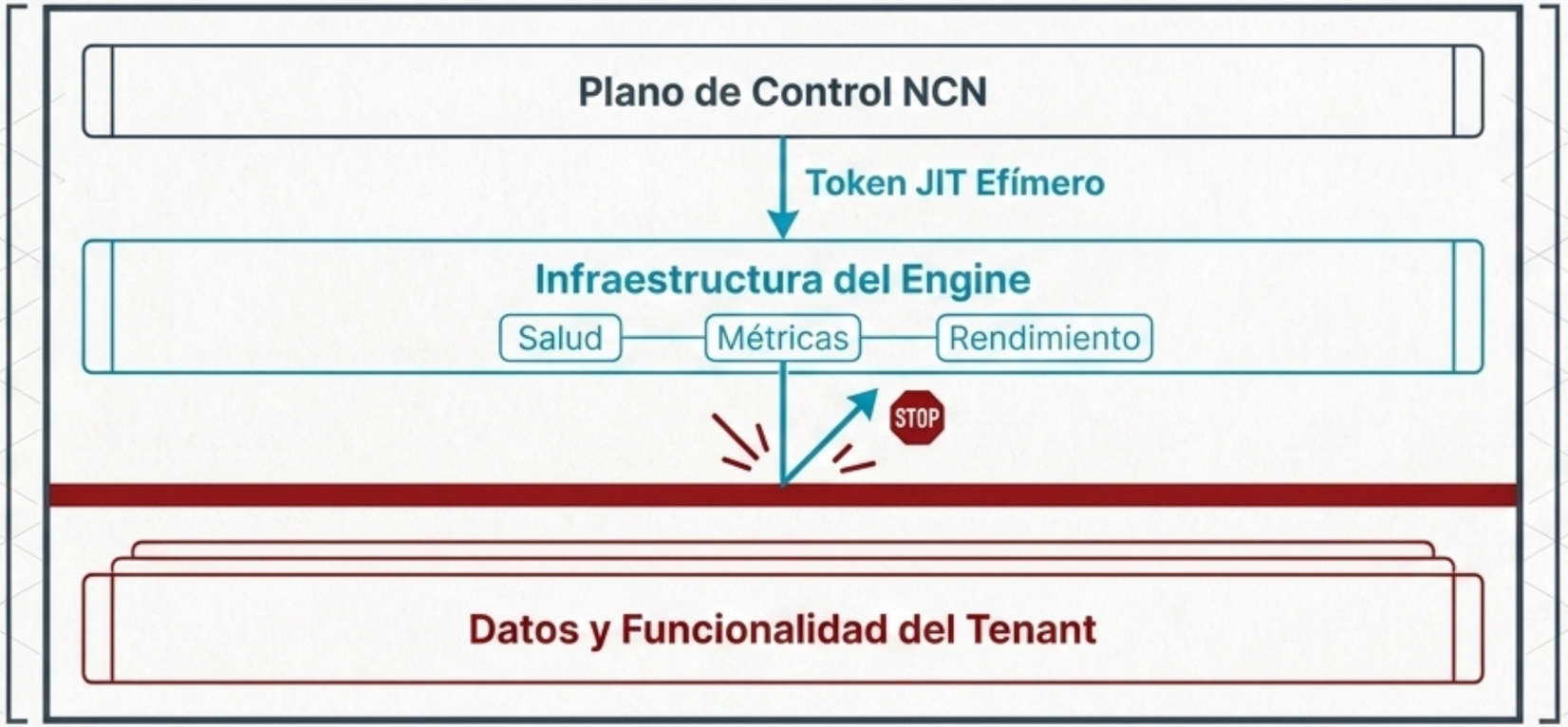
Concepto: Dual-control y *'two-person integrity'* (reducción de privilegio permanente).

Regla: Quórum mínimo 2/5 (2 de 5 Owners).

Mecanismo: Validación server-side. La operación queda pendiente hasta la aprobación explícita desde sesiones independientes.

Aplicación: Mutaciones raíz, acciones irreversibles, break-glass, cambios estructurales de plataforma.

Acceso NCN Efímero y Aislamiento de Datos



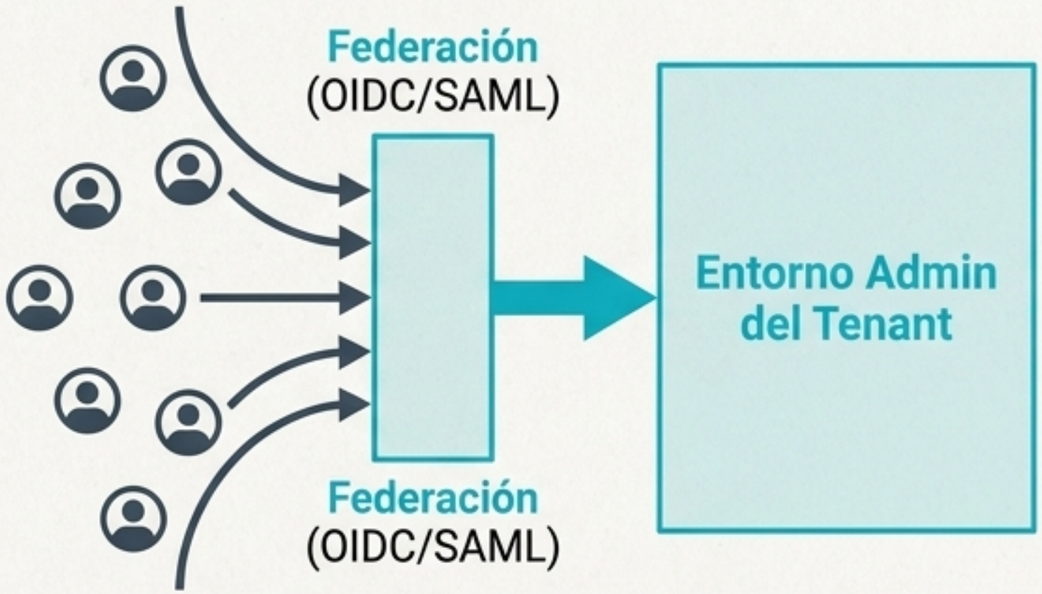
Just-In-Time (JIT):
Token temporal, scope limitado, TTL corto. Requiere PIM y justificación explícita.

Acceso Permitido:
Salud del Engine, métricas, diagnóstico, conectividad.

Barrera Hermética:
El token NO permite acceso a datos del tenant, auditoría raw, ni bypass de consentimiento.

Shell Administrativo vs. Autonomía de Aplicaciones

Autenticación Administrativa



Las aplicaciones integradas reutilizan el Plano de Acceso como shell administrativo unificado.

Aplicaciones con Usuarios Externos

Mantienen autonomía total sobre el login, sign-up y gestión de sesiones de sus clientes finales y externos.

Principio: La administración centraliza la identidad en la plataforma; el runtime final de la aplicación pertenece a su propio modelo de negocio.

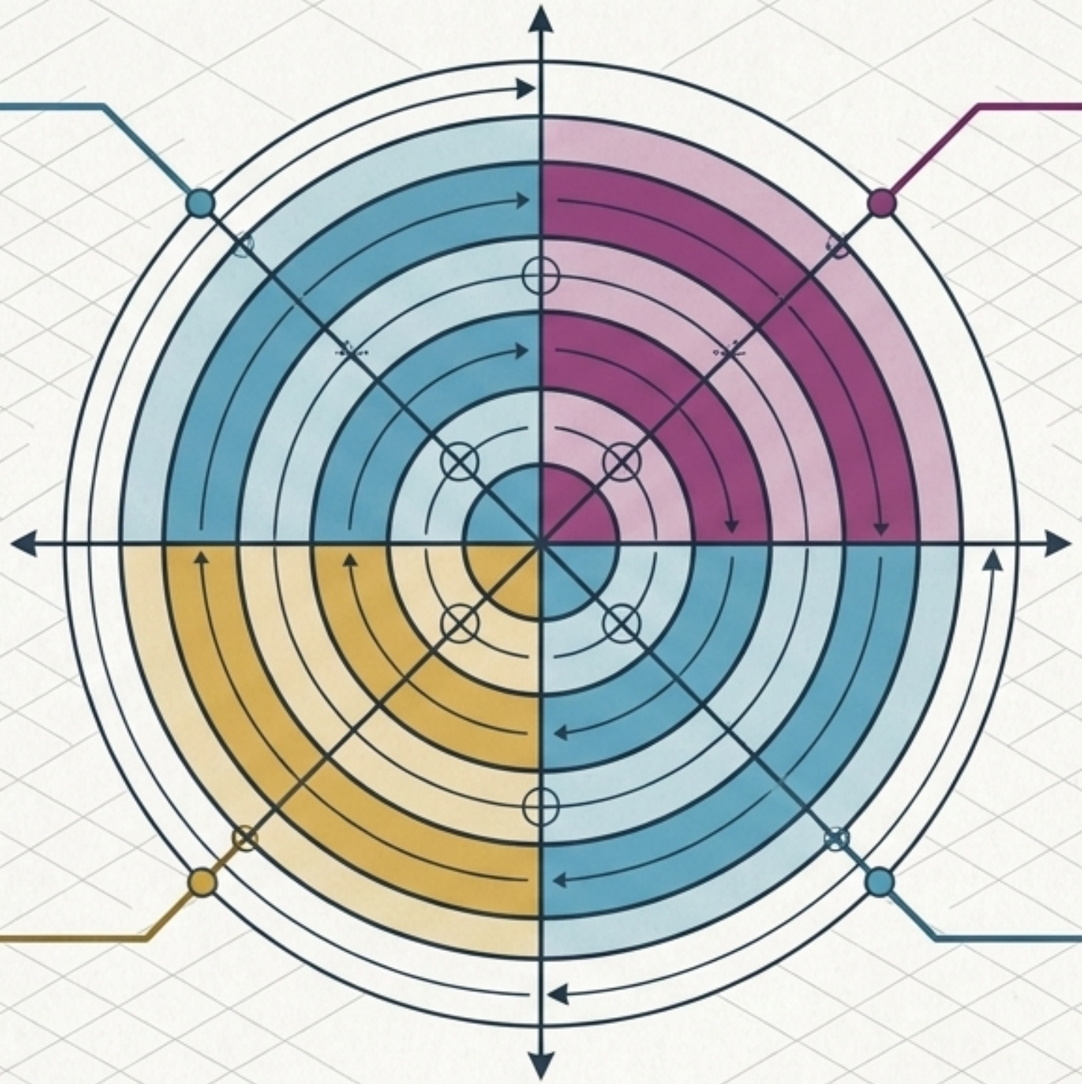
Capas Defensivas y Postura de Resiliencia

Protección de Sesión

Cookies JWE sealed, tokens ticket+exchange (fuera de URLs), dual-key rolling, TTL corto.

Anti-Abuso

Rate limiting global, protección CSRF, anti-user enumeration, anti-bcrypt-DoS.



Integridad de Credenciales

Detección de contraseñas comprometidas (HaveIBeenPwned k-anonymity), revocación distribuida.

Roadmap de Evolución

FIDO2, Passkeys, WebAuthn, Risk-based & Continuous authentication, Device fingerprinting.

El Ecosistema de Seguridad Integral

Síntesis: La autenticación (D05) inyecta la identidad en un sistema donde la capacidad es filtrada, gobernada y registrada implacablemente.

Conclusión Arquitectónica

SkyDefended InfraApp separa autenticación, confianza y autorización: los usuarios se autentican mediante mecanismos soberanos o federados; los Engines establecen confianza mediante identidad criptográfica distribuida; y toda capacidad efectiva se gobierna a posteriori bajo principios explícitos de Zero Trust.

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS