ENKIDU

— MIOVSKI GROUP —

ARQUITECTURA CONCEPTUAL

# Aegis Defence

La capa criptográfica resistente al cuántico de la pila Enkidu — establecimiento de claves poscuántico híbrido, firmas resistentes al cuántico y criptoagilidad a escala de flota, aplicada por Origi y operada por Helios Grid sobre el tejido Northwind.

Español · Edición resumida

Basada en la versión 0.1 · 4 de julio de 2026

Preparado por MIOVSKI GROUP

Clasificación · No clasificado · Borrador para revisión interna

La edición completa en inglés prevalece

# Acerca de esta edición

Este documento es una edición resumida, en español, de « Aegis Defence — Conceptual Architecture », versión 0.1 (4 de julio de 2026), preparada por Miovski Group. Cada sección del original está representada de forma abreviada. En caso de divergencia, la edición completa en inglés prevalece. Clasificación: no clasificado — borrador para revisión interna.

# Resumen

Toda promesa de la pila Enkidu descansa, en última instancia, en la criptografía. La cadena de custodia de Origi son firmas; la admisión de artefactos de Helios Grid son firmas; cada enlace de la malla, cada radio de retaguardia y cada canal de control es un intercambio de claves. Hoy esas primitivas — acuerdo de claves de curva elíptica y firmas clásicas — son seguras. Frente a un ordenador cuántico criptoanalíticamente relevante, no lo son: el algoritmo de Shor las rompe por completo, y el ataque « cosechar ahora, descifrar después » significa que el tráfico grabado hoy en un enlace de retaguardia podrá leerse retroactivamente el día en que exista tal máquina. Para un tejido que porta datos Protected B con sensibilidad de varias décadas, la amenaza cuántica no es un problema futuro — es un problema de grabación presente.

Aegis Defence es la respuesta de Enkidu: el marco criptográfico resistente al cuántico de la pila, y su cuarto marco fundamental. Donde Tangram da al tejido su estructura, Origi su confianza en ejecución y Helios Grid su operabilidad, Aegis le da su longevidad criptográfica — establecimiento de claves poscuántico híbrido en cada enlace, firmas resistentes al cuántico en cada artefacto y registro de custodia, y una criptoagilidad concebida como operación de flota y no como proyecto de reingeniería.

Aegis es deliberadamente conservador y deliberadamente ceñido a las normas. Su suite de algoritmos es el conjunto NIST finalizado — ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205), con HQC como reserva basada en códigos y LMS/XMSS para la firma de firmware — desplegado en construcciones híbridas según la práctica IETF, alineado con CNSA 2.0 para los niveles de defensa y con el calendario ITSM.40.001 de Canadá para los sistemas gubernamentales. Es implementable hoy en el hardware exacto que Northwind despliega: bibliotecas PQC embebidas optimizadas para ARM en los niveles de nodo y concentrador Jetson, y el SDK cuPQC de NVIDIA para verificación por lotes acelerada por GPU en los centros de fusión Grace-Blackwell. Y rechaza explícitamente la distribución cuántica de claves (QKD) para este tejido, en línea con la orientación aliada de seguridad nacional.

Una frase porta el diseño: híbrido por defecto, ágil por construcción, y nada confiado a matemáticas que un ordenador cuántico sabe romper.

# 1. Propósito y alcance

Esto es una arquitectura conceptual, no un manual de implementación ni una especificación criptográfica: define la estructura de Aegis, su suite de algoritmos, sus vínculos de protocolo y sus contratos con los demás marcos Enkidu. El despliegue de referencia es Northwind — la versión más difícil del problema: enlaces disputados y pobres en ancho de banda, clasificación de seguridad, anfitriones desde un nodo Jetson a batería hasta un centro de datos Grace-Blackwell, y datos cuya sensibilidad excede cualquier horizonte cuántico creíble. La misma arquitectura, con perfiles de parámetros civiles, es la capa criptográfica de Lamassu, de Helios Grid y de todo despliegue Enkidu.

Aegis no es un nuevo plano de componentes sobre el tejido; es la sustancia criptográfica de los planos existentes. El régimen de comunicaciones seguras de Origi, su cadena de custodia y sus controles de admisión son algoritmos Aegis; las identidades de enrolamiento de Helios, su estado deseado firmado y sus runbooks firmados son firmas Aegis. Aegis define la suite, los vínculos y la disciplina de cambio; Origi los aplica en cada frontera; Helios los distribuye a cada nodo. Lo que Aegis no es: nada de custodia centralizada de claves, nada de primitivas propias, nada de algoritmos sin normalizar — en criptografía, la novedad es riesgo.

## 2. La amenaza cuántica y los mandatos

Qué se rompe y qué no: un ordenador cuántico ejecutando Shor rompe por completo la criptografía de clave pública actual — RSA, Diffie-Hellman de curva elíptica, ECDSA. Grover solo debilita la criptografía simétrica de forma cuadrática, lo que se responde con el tamaño de clave: AES-256 y las familias SHA-2/SHA-3 siguen siendo seguras. La consecuencia precisa para la pila: todo intercambio de claves y toda firma deben migrar; el cifrado simétrico y el hashing requieren disciplina de parámetros, no sustitución.

La urgencia es asimétrica: una firma falsificada en el futuro no falsifica retroactivamente el pasado; pero un intercambio de claves roto en el futuro expone retroactivamente todo lo que protegía. Un adversario que hoy graba el tráfico de retaguardia de Northwind no necesita ningún ordenador cuántico — solo paciencia y almacenamiento. Por eso la primera ola de Aegis son KEM híbridos en los enlaces, no firmas. Y la transición ya no es especulativa: el NIST publicó las normas finalizadas en agosto de 2024, HQC fue seleccionado en marzo de 2025 como KEM de reserva basado en códigos, y FN-DSA (FIPS 206) está en desarrollo — una diversidad deliberada entre retículos, funciones hash y códigos.

- NSA (sistemas de seguridad nacional de EE. UU.) — CNSA 2.0 — ML-KEM-1024 y ML-DSA-87; LMS/XMSS para firma de código; QKD explícitamente excluida; migración por clases de producto hasta comienzos de los años 2030.
- CSE / Centro Canadiense de Ciberseguridad — ITSM.40.001 + SPIN del TBS — planes ministeriales para abril de 2026; sistemas de alta prioridad migrados a finales de 2031; todos los sistemas a finales de 2035; los algoritmos vulnerables « deshabilitados, aislados o tunelizados ».
- NCSC (Reino Unido) — calendarios de migración PQC — descubrimiento y planificación ahora; migración completa para 2035.

Un Northwind desplegado para las Fuerzas Armadas canadienses queda bajo la lectura más estricta de los tres: Aegis toma por ello los parámetros CNSA 2.0 como perfil techo y el ITSM.40.001 como calendario vinculante. El horizonte del mandato no es la fecha de llegada del ordenador cuántico: es la paciencia del adversario que graba, restada de la vida útil de sus datos.

## 3. Premisa de diseño e invariantes

Aegis descansa en una frase: híbrido por defecto, ágil por construcción, y nada confiado a matemáticas que un ordenador cuántico sabe romper. Híbrido, porque los algoritmos poscuánticos son jóvenes y los clásicos están condenados por el cuántico — combinarlos hace que la sesión sobreviva al fallo de cualquiera de los dos. Ágil, porque la única certeza de un campo joven es el cambio: algoritmos, parámetros y puntos de código se moverán, y una flota de diez mil nodos debe seguirlos como tarea de operaciones, no como reconstrucción.

- 01 · Solo normas — cada algoritmo de la suite es una norma NIST finalizada o una reserva explícitamente designada del proceso NIST. Ninguna primitiva propia, jamás.
- 02 · Híbrido hasta mandato en contrario — el establecimiento de claves combina un intercambio clásico con un KEM poscuántico (p. ej. X25519 + ML-KEM-768); los modos puramente PQC solo se activan donde un mandato lo ordena.
- 03 · La diversidad de algoritmos se mantiene en reserva — tras cada primario, una reserva sobre matemáticas distintas — HQC tras ML-KEM, SLH-DSA tras ML-DSA — preintegrada, para que una sorpresa criptoanalítica sea un cambio de política, no un programa de crisis.
- 04 · La política criptográfica es un artefacto firmado — la suite activa, los parámetros y los vínculos por segmento de flota se declaran en un artefacto de criptopolítica versionado y firmado, distribuido por Helios Grid y admitido por Origi como cualquier artefacto.
- 05 · La capa simétrica se dimensiona, no se sustituye — AES-256 y SHA-2/SHA-3 (384 bits o más en los niveles superiores) se conservan; a Grover se responde con tamaño de clave y de resumen.
- 06 · Nada se retira sin estar tunelizado — los algoritmos clásicos se retiran solo según la disciplina del mandato — deshabilitados, aislados o tunelizados dentro de una capa resistente al cuántico — nunca dejados en silencio en una ruta de respaldo.

¿Por qué no esperar? Dos argumentos cierran la cuestión: el ataque « cosechar ahora, descifrar después » — los datos que hoy se graban ya están perdidos o a salvo según lo que hoy los proteja — y la aritmética del calendario: la fecha canadiense de alta prioridad es finales de 2031, la fase 1 de Northwind se despliega en la misma ventana, y una capa criptográfica añadida tras el despliegue cuesta un múltiplo de una diseñada desde el inicio. Aegis existe para que Northwind nunca entregue un enlace vulnerable al cuántico.

# 4. La suite de algoritmos Aegis

La suite asigna a cada función criptográfica un algoritmo primario y una reserva, con parámetros perfilados por nivel de despliegue — perfil techo de defensa según CNSA 2.0, perfil estándar según el nivel 3 del NIST y las recomendaciones del Centro de Ciberseguridad para Protected B.

- Establecimiento de claves (enlaces, sesiones) — híbrido X25519 + ML-KEM-768 (estándar); híbrido con ML-KEM-1024 (techo defensa) — HQC en reserva basada en códigos; modo ML-KEM puro disponible donde se mandate.
- Firmas — custodia, telemetría, enrolamiento, veredictos — ML-DSA-65 (estándar); ML-DSA-87 (techo defensa) — SLH-DSA como reserva basada en hash, sobre matemáticas independientes.
- Firmas — firmware, cadena de arranque, imágenes BSP — LMS (SHA-256), XMSS — esquemas con estado, según la doctrina de firma de código de CNSA 2.0; compilaciones de solo verificación en nodos restringidos.
- Firmas — registro de artefactos (modelos, contenedores, políticas) — ML-DSA, con doble firma LMS para los artefactos de sistema base.
- Cifrado simétrico — AES-256 (GCM) — sin cambios; resistente al cuántico a este tamaño.
- Hashing / encadenado de custodia — SHA-384 / SHA-512, familia SHA-3 — estructura sin cambios; tamaños de resumen fijados por perfil.
- Certificados / PKI — cadenas ML-DSA; certificados híbridos durante la transición — cadenas clásicas tunelizadas en canales protegidos por Aegis hasta su retirada.

Dos omisiones deliberadas: FN-DSA (Falcon) se sigue pero no se adopta hasta que FIPS 206 se finalice — sus firmas compactas interesan a los enlaces más hambrientos de ancho de banda, y su lugar queda reservado — y ningún algoritmo fuera del proceso NIST aparece en parte alguna.

## 5. La arquitectura por capas

Aegis se materializa en cuatro puntos de enlace que ya existen todos en la pila — ese es el punto: Aegis es una sustitución de sustancia criptográfica, no una adición de piezas móviles. Protección de enlaces: cada enlace del tejido y cada canal de control de Helios pasa a TLS 1.3 con el grupo híbrido X25519+ML-KEM-768, DTLS 1.3 para los portadores de malla orientados a datagramas, y SSH híbrido para la administración — el adversario que graba no gana nada. Identidad: las cadenas de certificados de nodos, Wardens, Cores y operadores pasan a ML-DSA, con certificados híbridos durante la ventana de transición; las claves privadas residen en hardware donde el nivel lo permite.

Integridad: la cadena de custodia de Origi se firma con ML-DSA y resúmenes de clase SHA-384, con SLH-DSA disponible por política para los registros de mayor peso probatorio; los artefactos de Helios se firman con ML-DSA en el registro y se verifican en el nodo en el momento de la admisión — la verificación corre siempre en la última frontera de confianza antes del uso. Arranque: un tejido resistente al cuántico arrancado por un cargador falsificable cuánticamente es una contradicción — la cadena de arranque se firma con los esquemas con estado basados en hash (LMS/XMSS); la ranura que falla la verificación Aegis es la ranura que nunca arranca. Aegis no añade componente alguno al tejido: cambia de qué está hecho cada apretón de manos, cada firma y cada comprobación de arranque.

# 6. Proyección sobre el tejido

Los costes de la PQC son asimétricos — el cómputo es casi gratis, el ancho de banda no — y los niveles del tejido son asimétricos en sentido contrario. Aegis explota ambos.

- Nodo FIB (clase Jetson Orin) — PQC en CPU sobre los núcleos ARM: bibliotecas embebidas ML-KEM/ML-DSA optimizadas en ensamblador ARM, LMS/XMSS de solo verificación; (D)TLS 1.3 híbrido en cada enlace. Los apretones de manos de un nodo cuestan milisegundos de CPU por hora.
- Concentrador FIB (clase Thor) — la misma pila de CPU, más los deberes de concentrador: terminación de docenas de sesiones, verificación de las firmas de telemetría de los nodos, refirma de agregados — cómodamente dentro del presupuesto de CPU; la GPU queda dedicada a la inferencia.
- FOB-IFC (clase GB300) — entra cuPQC: verificación ML-DSA por lotes, acelerada por GPU, para los flujos de custodia y telemetría a escala de teatro, y operaciones ML-KEM por lotes para la gestión de sesiones sobre docenas de concentradores.
- Central IFC (clase NVL72) — despliegue completo de cuPQC vía la integración liboqs: infraestructura de firma del registro, verificación por lotes a escala de flota (millones de operaciones por segundo y GPU), servicios de ciclo de vida de claves, cadena de autoría de la criptopolítica.

# 7. Criptoagilidad — la criptografía como artefacto gestionado

La lección más profunda de la última década de criptoanálisis — incluido el colapso súbito, en 2022, de un candidato NIST de cuarta ronda ante un ataque clásico — es que la confianza en matemáticas jóvenes puede fallar de golpe. La respuesta de Aegis: hacer del cambio de criptografía una operación de flota rutinaria. La suite activa se declara por segmento en un artefacto de criptopolítica firmado y versionado, distribuido por Helios exactamente como un modelo: olas escalonadas, puertas de salud (tasas de éxito de los apretones de manos, interoperabilidad con la política anterior), reversión automática, custodia íntegra. Cambiar una flota de ML-KEM-768 a ML-KEM-1024 — o, en el escenario sorpresa, de ML-KEM a HQC — es un despliegue, no un programa.

Todo mandato empieza por el descubrimiento: no se migra lo que no se ha inventariado. En la pila Enkidu eso es casi gratis — el gemelo de nodo de Helios ya registra cada artefacto y vínculo instalados, de modo que el inventario criptográfico de la flota (CBOM) es una consulta sobre los gemelos, no una auditoría manual. Y la migración solo se completa cuando el algoritmo vulnerable ha desaparecido de la negociación: primero pierde su condición de predeterminado, luego se confina a interfaces heredadas tunelizadas tras canales protegidos por Aegis, y por último se retira de la compilación — cada paso, un despliegue de flota con rastro de custodia, de modo que « demuestre que RSA ha desaparecido » se responde desde el registro.

## 8. Dimensionamiento y rendimiento en enlaces disputados

El verdadero impuesto de la PQC sobre Northwind son los bytes, no los ciclos — y muerde en los portadores de malla. Una clave pública/un cifrado ML-KEM-768 pesan ~1,2/1,1 KB (frente a 32 bytes de X25519), pagados una vez por apretón de manos; una firma ML-DSA pesa de 2,4 a 4,6 KB (frente a 64-72 bytes de ECDSA), pagada por registro firmado — el coste recurrente dominante; SLH-DSA, de ~7,9 KB en adelante, queda reservada a los registros de mayor peso probatorio y a los roles de firmware.

Tres mitigaciones lo mantienen dentro de las envolventes del tejido: la amortización de los apretones de manos — las sesiones de malla son largas y reanudadas, y se amortizan sobre horas de vida del enlace; la agregación de firmas en el concentrador — los nodos firman a nivel de registro, los concentradores verifican localmente y reenvían agregados firmados por ellos, de modo que las firmas individuales no transitan el enlace de retaguardia — lo que se compone exactamente con la reducción « señal, no datos » de Helios; y la reserva de firmas compactas — el lugar de FN-DSA existe para los portadores más restringidos en cuanto FIPS 206 se finalice. El sobrecoste residual pasa a ser un dato de entrada de la aritmética de envolventes de telemetría de Helios, y no una sorpresa descubierta en el campo.

## 9. La posición sobre la distribución cuántica de claves

Aegis toma una posición nítida: nada de QKD en este tejido. Las razones son las de las agencias aliadas, y son arquitectónicas: la QKD exige equipos ópticos dedicados — una solución de hardware donde la PQC es de software; es inadecuada para las comunicaciones móviles y tácticas y para cualquier ruta con relés fuera del control de la organización; distribuye claves pero no autentica, dependiendo así de firmas de nivel PQC de todos modos; y concentra un riesgo de denegación de servicio en un canal saturable. La NSA no respalda la QKD para los sistemas de seguridad nacional y CNSA 2.0 la excluye. Queda anotado un punto de vigilancia: los enlaces fijos estratégicos punto a punto entre sedes permanentes del Central IFC son el único nicho donde existen despliegues de QKD (el programa canadiense QEYSSat explora la QKD satelital); si la política cambiara, tal enlace entraría como una fuente de claves más bajo la derivación híbrida de Aegis — una capa adicional, nunca un sustituto, y nunca en el tejido táctico.

## 10. Correspondencia de cumplimiento

Cada requisito de los mandatos se traza hasta su mecanismo: ML-KEM-1024/ML-DSA-87 para sistemas de clase NSS mediante el perfil techo de la criptopolítica; LMS/XMSS para firma de código mediante los roles de arranque; la exclusión de la QKD por la posición de la sección 9; los planes de migración e informes anuales desde abril de 2026 mediante el CBOM derivado de los gemelos y el historial de versiones de la política; la fecha de 2031 mediante la primera ola híbrida en todos los enlaces; « deshabilitado, aislado o tunelizado » mediante la disciplina de retirada; y la migración completa de 2035 mediante la convergencia de política a escala de flota, verificada desde los gemelos y las trazas de custodia.

## 11. Madurez y camino a seguir

La entrega se alinea con las fases de Northwind y Helios Grid y con el reloj de los mandatos. Fase 1: establecimiento de claves híbrido en cada enlace y canal de control; firma ML-DSA para custodia, telemetría y artefactos; cadena de arranque firmada con LMS; primer artefacto de criptopolítica y CBOM de referencia — resultado: ningún intercambio de claves vulnerable al cuántico en el tejido desplegado. Fase 2: perfil techo de defensa para los segmentos designados; verificación por lotes cuPQC en el FOB-IFC; certificados híbridos en toda la flota; opción SLH-DSA; retirada de la negociación puramente clásica. Fase 3: servicios centrales de ciclo de vida de claves y firma de registro sobre cuPQC/liboqs; adopción de FN-DSA para los portadores restringidos al finalizarse FIPS 206; algoritmos clásicos retirados de las compilaciones; informe de cumplimiento continuo. Las cuestiones abiertas — selección de módulos validados FIPS por nivel, custodia de claves en hardware, perfiles de certificados híbridos, cobertura de plataforma de cuPQC — quedan registradas como compromisos para el diseño detallado.

# Conclusión

Tangram hizo legibles los tejidos Enkidu; Origi los hizo defendibles; Helios Grid los hizo operables. Aegis Defence los hace duraderos — capaces de prometer que lo que la flota cifra, firma y arranca hoy seguirá siendo confidencial, auténtico y confiable cuando el ordenador del adversario ya no sea clásico.

Su contribución es disciplina antes que invención: una suite compuesta solo de normas finalizadas, con una reserva sobre matemáticas independientes tras cada primario; un establecimiento de claves híbrido donde la juventud y la obsolescencia se cubren mutuamente las debilidades; firmas asignadas a los roles que los mandatos realmente distinguen; todo ello expresado como política firmada que Helios despliega y Origi aplica, de modo que cambiar la criptografía sea una operación de flota auditada; y una negativa rotunda a gastar el peso y el dinero del tejido en hardware cuántico que la misión no puede usar.

Híbrido por defecto. Ágil por construcción. Nada confiado a matemáticas que un ordenador cuántico sabe romper.