FORWARDEDGE

OCTANS SPACE AFRICA

Isidore Quantum®: Solución Integral de Ciberseguridad y Criptografía Poscuántica

INTRODUCCIÓN COMERCIAL

Fecha: ABRIL 2026

Forward Edge-AI, Inc. | Octans Space | www.octanspace.com | forwardedge.ai
América Latina POC: octans@inhub.world

PROBLEMA: Las organizaciones retrasan la adopción de PQC, dejando los datos críticos expuestos a las brechas actuales y a las amenazas cuánticas del mañana.

- **Riesgo Inmediato:** El cifrado actual ya es vulnerable a ciberataques avanzados impulsados por IA y patrocinados por Estados.
- **Harvest-Now, Decrypt-Later:** Los adversarios están capturando datos cifrados hoy para su descifrado futuro mediante computación cuántica.
- **Inminencia Cuántica:** Los avances cuánticos pueden llegar antes de lo esperado—haciendo que el retraso en la adopción de PQC sea una responsabilidad crítica

> "There is nothing in our portfolio that is high assurance, low cost, easy to own, future proof, easy to certify, scalable to multiple form factors, and non-Controlled Cryptographic Item (CCI)"
>
> Andy White
> National Security Agency, June 2022

60%
Las organizaciones globales experimentaron una brecha de datos.

US$4.9M
Costo promedio de una brecha de datos.

80%
El tráfico cifrado puede ser capturado y almacenado para descifrado futuro.

70%
Los líderes de seguridad de nivel ejecutivo reconocen que no tienen un plan de transición post-cuántica.

<5
Años antes de que los computadores cuánticos puedan romper RSA-2048 y ECC.

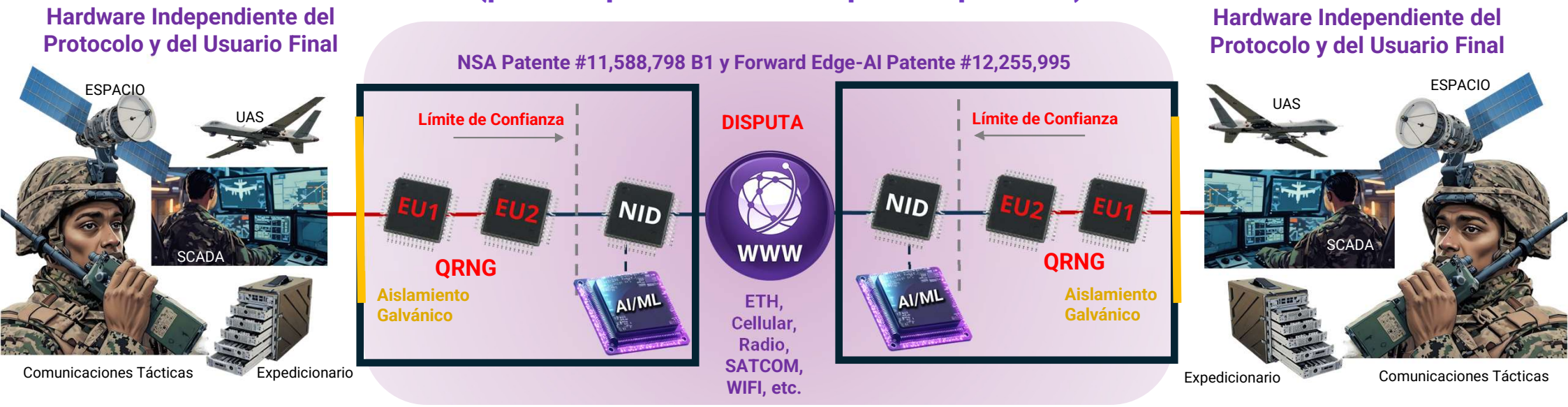
SOLUCIÓN: Isidore Quantum®

Isidore Quantum® es una plataforma todo-en-uno de ciberseguridad y cifrado post-cuántico que unifica defensa Zero-Trust, respuesta autónoma a amenazas y criptografía preparada para el futuro en una sola solución drop-in. Diseñada para redes comerciales, gubernamentales y militares por igual, protege datos críticos y comunicaciones contra los ciberataques avanzados actuales y las amenazas cuánticas del mañana—sin requerir cambios costosos en la infraestructura:

- **Protección Integral:** Unifica ciberseguridad y cifrado post-cuántico en una solución escalable y lista para implementar.
- **Seguridad Preparada para el Futuro:** Defiende datos sensibles de los ataques impulsados por IA actuales y de las amenazas de descifrado cuántico del mañana.
- **Integración Sin Interrupciones:** Se instala fácilmente en infraestructuras IT y cloud existentes—no requiere rediseño costoso.
- **Inteligencia Autónoma:** El monitoreo impulsado por IA detecta y neutraliza amenazas en tiempo real sin intervención humana.
- **Eficiencia de Costos:** Reduce el gasto en ciberseguridad hasta en un 60% mediante protección unificada y gestión automatizada de claves.

Cómo Funciona

(punto a punto mostrado por simplicidad)



Isidore es un dispositivo de cifrado seguro frente a la computación cuántica y ciberseguridad en **cumplimiento con la NSA CNSA 2.0** que protege los datos mediante hardware seguro y un diseño Zero Trust, eliminando la necesidad de infraestructuras tradicionales de claves. Al combinar cifrado AES-256 con ML-KEM, y el Generador Cuántico de Números Aleatorios (QRNG) de Quantinuum, el sistema produce claves de cifrado verdaderamente impredecibles. Operando en Capa 2, el dispositivo crea enlaces de red seguros y flexibles que soportan configuraciones punto a punto, hub-and-spoke y malla. El Dispositivo de Interfaz de Red (NID) aplica separación física y lógica red/black entre zonas confiables y no confiables, mientras que la Inteligencia Artificial (IA) integrada monitorea el tráfico, identifica amenazas y se adapta en tiempo real para mantener la continuidad de la misión. El despliegue ocurre un 70% más rápido y el costo total de propiedad es un 60% menor que con soluciones convencionales, entregando una plataforma unificada y resiliente a lo cuántico para uso comercial y de defensa.

DIFERENCIACIÓN

Criteria	Isidore Quantum® - Todo-en-Uno	QKD	PQC Solo Software
Costos de Integración	**~USD$700/mes por enlace** Drop-in, sin re-arquitectura	**USD$100K+ por enlace** Requiere fibra dedicada, óptica o satélites	**Bajo costo inicial, con costos ocultos** En parches, latencia y gestión
Costo Total de Propiedad (En 5 años)	**60%** Menor que cifradores legacy; Amigable para OPEX	**Más Alto** Escala limitada, el costo crece exponencialmente con la distancia y nodos	**Moderado** Barato de desplegar, costoso de mantener debido a parches y fallas
Rendimiento en Sistemas Legacy	**<0.5ms Latencia** Funciona sin problemas con IPv4/IPv6, SCADA, radio, SATCOM	**Deficiente** Limitado por distancia;Incompatible con sistemas legacy y móviles	**Débil** Degrada el rendimiento en hardware limitado / legacy; añade latencia
Riesgos de Seguridad	**Mínimo** Aislamiento hardware Red/Black, claves efímeras, resiliencia impulsada por IA	**Frágil** Se rompe ante interrupciones físicas;Vulnerable a pérdida de canal	**Alto** Gran superficie de ataque, riesgos de canales laterales, dependencia de parches
Capacidad Drop-in	**Excelente** Agnóstico a protocolo / hardware; Conectar y asegurar inmediatamente	**Deficiente** Requiere fibra personalizada; Impráctico más allá de pilotos	**Inconsistente en redes mixtas** A pesar de ser bueno en teoría
Preparación para Acceso Móvil (1)	✓	✗	✗

(1) Isidore cumple con los requisitos del paquete de capacidad de acceso móvil CSfC de la NSA (MACP), que describe cómo proteger datos móviles clasificados en tránsito usando algoritmos criptográficos aprobados.

VARIANTES

Isidore 1 – SCADA/OT, IoT

Isidore 50 MB/s – 2 GB/s

One Way Data Diode

Isidore Quantum 1701 - Enterprise

	50 Mb/s	480 Mb/s	1 - 2 Gb/s	10 Gb/s	68 Gb/s	1 Tb/s
Tamaño, Peso y Potencia	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~7 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~10 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~12 W	Disponible Q3 2026	Disponible Q3 2026	Disponible Q4 2026
Ambiental	–40 °C a +85 °C; calificado para choques y vibraciones.					
Criptografía	AES-256 GCM y ML-KEM					
Entropía Cuántica	Subsistema integrado de Generador de Números Aleatorios Cuánticos (QRNG); validado según NIST SP 800-90 A/B/C y BSI AIS-31.					
Topologías	Punto a punto, punto a multipunto, malla y hub-and-spoke; compatible con topologías cableadas, inalámbricas e híbridas.					
Certificaciones y Cumplimiento	NSA CNSA 2.0, FIPS 140-3 (Nivel 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (Excepción de Licencia ENC)					
Latencia	<90 µs (estimado)					
Arquitectura de Seguridad	Separación Rojo/Negro (Red/Black) aplicada por hardware con aislamiento galvánico; operación de confianza cero (zero-trust) y sin intervención (zero-touch); postura encubierta (sin anuncios de red ni respuestas a sondas)					
IA / Autonomía	Motor de IA embebido entrenado para la detección de anomalías en tiempo real y respuesta auto-reparadora.					
Sistema de Gestión	Cassian™ para la orquestación de flotas, aprovisionamiento, telemetría y gobernanza de políticas en implementaciones distribuidas.					

23 PRUEBAS DE CONCEPTO EXITOSAS: Aire, Espacio, Tierra y Mar

VALIDACIÓN: SCADA/OT – USAF FASE 2 SBIR

- Una plataforma de ciberseguridad resistente a la computación cuántica para entornos ICS/SCADA, OT e IoT (US Air Force 688th Cyberspace Wing).
- Permite la aplicación de zero-trust, cifrado de extremo a extremo y acceso basado en roles en la capa física sin depender de PKI.
- Soporta hot-patching, detección de anomalías mediante ML y actualizaciones seguras de firmware sin interrumpir las operaciones.
- Integra analítica consciente de OT con SIEM para obtener insights de seguridad correlacionados a través de dominios IT/OT.
- Diseñada para contrarrestar amenazas “Harvest Now, Decrypt Later” (HNDL) y futuros ataques cuánticos.

FLC
Fede a Laberstory Consortium
Tor Technology- Tansfer

TECH | SBIR AUTONOMY
WINNER

AFWERX
CHALLENGE

ESPACIO: USAF Y USSF FASE II SBIRS

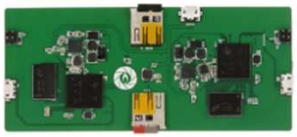
- **Isidore Quantum** fue seleccionado como la columna vertebral del router espacial de alto rendimiento que integra enrutamiento resistente a la computación cuántica en constelaciones LEO (US Space Force Proliferated Warfighter Space Architecture (PWSA)).
- **Isidore Quantum** fue seleccionado como un dispositivo criptográfico de alto rendimiento, multidominio y punto a multipunto para PWSA.
- **Isidore Quantum** se encuentra actualmente en órbita en una prueba de concepto de Seguridad de Comunicaciones Espaciales (Space COMSEC) de la Fuerza Aérea de los Estados Unidos.

ANTECEDENTES/HISTORIA: Orígenes en la NSA como teléfono seguro para el Presidente de los Estados Unidos.

El Dispositivo de Cifrado Libre de Protocolo (PFED) fue desarrollado por la NSA para crear un sistema de comunicación seguro e independiente de protocolos que protege la voz y los datos del Presidente sin depender de infraestructuras complejas de PKI o VPN. Diseñado para simplicidad y modularidad, PFED utiliza hardware comercial en una arquitectura única que logra alta seguridad y cumple con los estándares CNSA 2.0. Al separar el cifrado de los protocolos de red, PFED elimina vulnerabilidades presentes en transiciones post-cuánticas basadas en software y proporciona una solución resiliente tipo drop-in para liderazgo nacional y operaciones de defensa. Las ventajas clave del PFED incluyen:

- **Cumplimiento CNSA 2.0**
- **Diseño "Drop-In" de Protocolo Agnóstico**
- **Superficie de Ataque Minima**
- **Gestión Autónoma de Claves**
- **Integración con Hardware Comercial**
- **Ítem Criptográfico No-Controlado (Non-CCI)**

INVENTADO POR LA NSA Y RESPALDADO POR 3 AÑOS DE I+D FINANCIADOS POR USAF Y USSF: TRL 8 en Diciembre 2024



TRL 2 - PFED
(2018 - 2020 NSA)

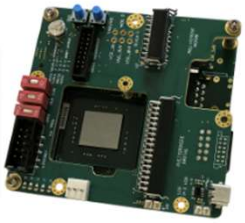
- Módulos Beagle Bone y Raspberry Pi
- Pruebas F35, sUAS, REAPER
- Pruebas CYBERCOM
- Instalación/pruebas OT/SCADA de la NSA

TRL 3 - Isidore
(2022 CRADA)

- Procesador ARM simple
- Interfaces USB, ETH, WIFI
- Simulaciones y pruebas en laboratorio
- La NSA recibe patente para PFED

TRL 6 - Isidore
(2023 Fase I SBIRs)

- Procesador ARM Mejorado
- Interfaces USB, ETH, WIFI
- 1,000(+) entrevistas estructuradas con stakeholders
- Rendimiento de 50 Mb/s
- Pruebas en smartphones y comunicaciones expedicionarias
- Simulaciones y pruebas en laboratorio
- Pruebas de laboratorio (Lumen)



TRL 7/8 - Isidore
(2024 Fase II SBIRs)

- Versión espacial COMSEC
- 100 Mb/s / nuevo procesador
- Premio PWSA crypto espacial de alto rendimiento
- Premio PWSA router espacial de alto rendimiento
- Endurecimiento contra radiación
- Premio Air Force CSO
- Victorias AFGSC y Army Challenge
- Pruebas AFSOC, AFNWC, Idaho Labs, Lumen, MITRE, CACI
- **Alcanzó TRL-8 en diciembre de 2024**

TRL 8 - Isidore
(2025 Fase II SBIRs)

- CubeSat lanzado
- Pruebas FCC
- FIPS 140-3
- Interfaces seriales y de radio• POCs en banca, marítimo, energía, Taiwán
- Nuevo procesador neuromórfico (800 Gb/s)
- Forward Edge-AI recibe múltiples patentes
- Ganador premio FLC
- US Army menor SWaP-C
- Cliente especial

TRL 8+
(Capital Privado)
(2025/2026)

- Compra NSB Taiwán
- NOMARS y Stiletto
- Bus estándar VITA 46.XX para JADC2/ABMS
- **CSfC (planificado)**
- **Alta seguridad (planificado)**
- Procesador neuromórfico
- Rendimiento 1 Tb/s
- Instalación Japan IPA
- 50 buques marítimos

ALGORITMOS CNSA 2.0: Compromisos Prácticos y Riesgos en Sistemas Legacy

AES-256 GCM sigue siendo la piedra angular de CNSA 2.0, ofreciendo una base de cifrado probada, resistente a lo cuántico y de bajo riesgo, ya bien integrada en sistemas DoD y OTAN. ML-KEM y ML-DSA son críticos para la migración post-cuántica pero introducen desafíos significativos de rendimiento e integración para infraestructura legacy. LMS/XMSS es adecuado para firma de firmware, mientras que SPHINCS+ es impráctico, destacando que AES ancla la seguridad actual mientras PQC proporciona la resiliencia necesaria frente a amenazas cuánticas futuras.

Algoritmo (CNSA 2.0)	Tasa de Error	Impacto en Ancho de Banda	Costo de Implementación	Impacto en Infraestructura Legacy	Conclusión Clave
ML-KEM (Kyber) – Intercambio de Claves	Despreciable (≈2^{-165} a 2^{-175})	Medio (~1–1.5 KB por handshake, mayor que ECC pero manejable)	Medio (actualización firmware/lib, sin aceleración HW en equipos antiguos)	Medio – puede romper límites MTU/buffer, ralentiza radios/routers sin aceleración.	El KEM PQC más práctico; eficiente pero con un mayor consumo de búferes/CPU legacy.
ML-DSA (Dilithium) – Firmas	Ninguna (determinista)	Alto (firmas 3–5 KB vs. ~64B ECDSA)	Alto (renovación smart card/embebidos; upgrades HW+firmware)	Alto – crecimiento de certificados, presión en almacenamiento/ancho de banda.	Firma PQC estándar; robusta pero con un alto impacto en la infraestructura de clave pública (PKI) legacy.
LMS/XMSS – Basado en Hash (Firma de Firmware/Código)	Ninguna (basado en hash; riesgo en seguimiento de estado)	Bajo–Medio (firmas de varios KB; uso poco frecuente)	Medio (requiere gestión de estado)	Bajo–Medio – aceptable por uso poco frecuente.	Ideal para la firma de firmware/código; sobrecarga manejable si se aplican controles de ciclo de vida.
SLH-DSA (SPHINCS+) – Basado en Hash (Sin Estado)	Ninguna (basado en hash)	Muy alto (8–50 KB firmas; 30–50× mayor que ECC)	Alto (coste CPU/memoria; verificación lenta)	Alto – impráctico en sistemas legacy	Seguro pero poco práctico; excluido del uso de CNSA 2.0 NSS.
AES-256 GCM – Cifrado Simétrico (Clásico, Aprobado CNSA 2.0).	Ninguna (determinista)	Bajo (tamaño de bloque fijo, sobrecarga despreciable)	Bajo (librerías disponibles; aceleración HW común)	Bajo: ya implementado en la mayoría de los sistemas del Departamento de Defensa/OTAN; fuerte soporte de hardware.	Cifrado simétrico resistente a la computación cuántica; "estándar de oro" para datos TS, eficiente con aceleración por hardware; las limitaciones de recursos solo importan en hardware muy restringido.

ENFOQUES SOLO DE SOFTWARE: Riesgos Inaceptables

El cifrado solo software es económico inicialmente pero presenta bajo rendimiento en sistemas tácticos legacy, introduce latencia y conlleva alto riesgo de seguridad debido a débil aislamiento red/black y exposición a ataques de canal lateral. Las soluciones solo hardware ofrecen alto rendimiento y fuerte aislamiento, pero con mayores costos. Los enfoques híbridos, como PFED, equilibran rendimiento y seguridad utilizando hardware comercial, siendo la opción más práctica para modernizar sistemas bajo CNSA 2.0.

Tipo de Solución	Rendimiento en Sistemas Legacy	Costo/Riesgo de Integración	Riesgos de Seguridad	Capacidad Drop-in
Solo software	La velocidad está ligada a la potencia de la CPU; el hardware antiguo genera un rendimiento deficiente y una alta latencia.	Bajo costo (instalación de software), pero alto riesgo de problemas de integración y carga pesada de la CPU.	No hay aislamiento rojo/negro; los errores del sistema operativo/aplicación o los canales laterales comprometen la seguridad.	Deficiente – requiere instalación en todas partes, no es transparente.
Solo Hardware	ASIC/FPGA puede funcionar a velocidad de línea, pero es muy caro; no se puede parchear si es ASIC.	Alto costo de adquisición y certificación; se requiere un nuevo dispositivo.	Fuerte aislamiento, pero el hardware de función fija limita la flexibilidad; los aceleradores vinculados al host no ofrecen aislamiento.	Bueno – es un verdadero encriptador en línea, pero costoso y rígido.
Híbrido (ej. PFED/Isidore)	Hasta ~500 Mbps en hardware estándar; optimizado para el borde táctico.	Coste moderado; integración más sencilla que el Tipo 1; se puede reparar con piezas estándar.	Garantiza la separación física Rojo/Negro con procesadores independientes; resistente a ataques de canal lateral; función de reinicio/puesta a cero automática integrada.	Excelente – fácil de usar, independiente del protocolo, requiere cambios mínimos.