FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum®

Solución Integral de Ciberseguridad y PQC de Fácil Integración

Dominando el Futuro: Ciberseguridad Resistente a la Computación Cuántica para la Superioridad Aérea y Espacial

¿Por qué Isidore Quantum?

Asequible: 70% más rápido de implementar y 60% menos del costo total de propiedad.

Resiliencia Cibernética Autónoma: un sistema impulsado por IA, detecta, se adapta y se autorrepara frente a amenazas en constante evolución.

Integración Sencilla: El diseño independiente del protocolo, el hardware y la interfaz moderniza las redes heredadas sin necesidad de renovar la infraestructura.

Ventaja Low-SWaP: Compacto, eficiente y escalable para uso en empresas, defensa e infraestructuras críticas.

Las redes militares y gubernamentales, que abarcan mando y control, inteligencia, logística e investigación, enfrentan ahora una convergencia de amenazas cibernéticas y cuánticas capaces de socavar la seguridad nacional en cuestión de segundos. La mayoría de los sistemas de defensa aún dependen del cifrado RSA y ECC, algoritmos que las computadoras cuánticas podrán romper instantáneamente una vez que alcancen capacidad operativa. Los adversarios ya están explotando esta vulnerabilidad mediante campañas de “Harvest Now, Decrypt Later” (HNDL), recopilando datos y comunicaciones de misión cifrados para descifrarlos en el futuro cuando la tecnología cuántica madure.

La RAND Corporation y el CIO del Pentágono han advertido que el “Q-Day” podría llegar dentro de cinco años—mucho antes de que los programas tradicionales de adquisición puedan entregar soluciones certificadas. La aversión al riesgo y la dependencia de grandes contratistas han ralentizado los esfuerzos de modernización, incluso mientras las intrusiones impulsadas por IA y los compromisos en la cadena de suministro continúan debilitando la confianza en las redes de defensa. Esperar sistemas Tipo 1 ideales que podrían tardar años en desplegarse representa un peligro mucho mayor que actuar ahora, ya que, en un conflicto habilitado por tecnología cuántica, el primer sistema en fallar probablemente será el de mando y control.

Isidore Quantum proporciona una solución inmediata, integral, de ciberseguridad y criptografía post-cuántica (PQC), diseñada para proteger las operaciones militares y gubernamentales frente a amenazas actuales y emergentes. Basada en algoritmos conformes con NSA CNSA 2.0, la plataforma integra detección de anomalías impulsada por IA, gestión autónoma de claves y una arquitectura de confianza cero en un sistema compacto y de bajo consumo, desplegable en entornos clasificados, tácticos y empresariales. Desarrollado con componentes comerciales (COTS) y validado mediante bancos de pruebas de la Fuerza Aérea, la Marina y la Fuerza Espacial, Isidore Quantum® ofrece seguridad equivalente a Tipo 1 a una fracción del costo y del tiempo de despliegue requeridos por los sistemas tradicionales.

Con un nivel de madurez tecnológica TRL 8, el sistema protege comunicaciones, enlaces de datos y redes de misión sin requerir rediseño de infraestructura, ofreciendo una defensa disponible hoy frente al descifrado cuántico, intrusiones cibernéticas y disrupciones del mando. En una era donde la velocidad, la asequibilidad y la resiliencia determinan la ventaja estratégica, Isidore Quantum® actúa como el puente crítico entre la infraestructura actual y una fuerza segura frente a amenazas cuánticas.

La Situación

312%

Aumento de intrusiones cibernéticas dirigidas a redes de la USAF

85%

De los sistemas de la USAF aún dependen de cifrado RSA o ECC

30%

De las redes críticas de misión de la USAF dependen de tecnología OT de 20 años de antigüedad

70%

De las intrusiones cibernéticas se rastrean a estados nación

Las fuerzas militares de EE. UU. y sus aliados enfrentan una convergencia cada vez más intensa entre la guerra cibernética y la computación cuántica que amenaza el núcleo de los sistemas de mando y control (C2), inteligencia y sostenimiento. Las directrices del Pentágono para 2025 identifican el descifrado cuántico como una “amenaza existencial” para las comunicaciones seguras y los datos de misión. Los análisis de RAND advierten que, una vez que los sistemas cuánticos adversarios alcancen plena capacidad, los métodos criptográficos actuales podrían colapsar en segundos, exponiendo órdenes clasificadas, información de objetivos y operaciones logísticas en todos los dominios.

A pesar de la urgencia, muchos líderes gubernamentales en ciberseguridad y adquisiciones continúan dudando, posponiendo la acción hasta que grandes contratistas de defensa entreguen soluciones de alta garantía que a menudo llegan años tarde y a un costo significativamente mayor. Las lecciones de la guerra en Ucrania muestran que la disuasión futura dependerá de sistemas desplegables rápidamente, asequibles y construidos con componentes comerciales capaces de escalar más rápido que los procesos burocráticos. Retrasar la adopción esperando soluciones “perfectas” desarrolladas en laboratorio dejará a las redes de defensa vulnerables y desprotegidas cuando surja el conflicto.

Isidore Quantum: Solución Integral de Ciberseguridad PQC

El ecosistema Isidore Quantum es un conjunto de soluciones de ciberseguridad y cifrado post-cuántico impulsadas por IA, diseñadas para proteger el mando y control militar, la logística y los sistemas espaciales frente a amenazas cibernéticas actuales y futuros ataques de descifrado cuántico. Mientras los adversarios ejecutan operaciones HNDL para capturar datos de misión cifrados y perturbar operaciones en entornos disputados, la suite Isidore ofrece una arquitectura de defensa “plug-and-play”, de confianza cero y conforme a CNSA 2.0, desplegable en todos los dominios.

Desde Isidore 1 y el Data Diode de Isidore, que aseguran redes tácticas e industriales, hasta Isidore Enterprise 1701 que protege centros de datos, y soluciones como Space COMSEC, HTSR y HTSC que refuerzan comunicaciones orbitales y satelitales, el ecosistema proporciona protección resiliente a nivel cuántico en todas las capas. Ligero, basado en COTS y probado en campo, Isidore Quantum® ofrece al Departamento de Defensa una vía asequible, escalable y preparada para el futuro para mantener la superioridad cibernética en la era cuántica.

Capacidad	Impacto en la Misión
Cifrado Post-Cuántico (CNSA 2.0)	Protege datos clasificados y tácticos frente a descifrado cuántico mediante ML-KEM y AES-256-GCM
Defensa Cibernética Impulsada por IA	Aprende los “patrones de vida” operativos, detecta intrusiones de forma autónoma y se autorrepara sin intervención humana
Confianza Cero por Diseño	Elimina PKI, certificados y cargadores de claves, reduciendo la carga cognitiva y logística de los operadores.
Bajo SWaP-C, Alto TRL	Consume aproximadamente 8W según la variante, construido con componentes COTS y validado en 23 entornos operativos (Fuerza Aérea, Marina y Fuerza Espacial).
Plano de Control CASSIAN	Gestión centralizada con visibilidad en tiempo real, aplicación de políticas y agilidad criptográfica en activos distribuidos.
Aislamiento Rojo/Negro y Entropía Cuántica	Segmentación impuesta por hardware + generación de ruido cuántico para claves verdaderamente aleatorias y de un solo uso.

Confiar únicamente en AES-256 crea una peligrosa ilusión de seguridad. El cifrado sigue siendo fuerte, pero la infraestructura que lo rodea ya se está desmoronando. Los algoritmos cuánticos romperán los intercambios de claves, los ataques de canal lateral extraerán secretos en tiempo real, y los exploits impulsados por IA se adaptarán más rápido que cualquier parche. Quienes se aferran a 'AES-256 es suficiente' corren el riesgo de proteger una bóveda vacía mientras los intrusos entran por puertas invisibles. La era que viene exige más que resistencia a la fuerza bruta; exige arquitecturas diseñadas para la resiliencia frente a la velocidad cuántica, las fugas físicas y adversarios con inteligencia artificial.

El Caso de Negocio para el Liderazgo

Las redes militares y gubernamentales ya no pueden permitirse esperar sistemas de cifrado "perfectos". Isidore Quantum® ofrece la alta garantía de los principios Tipo 1 a una fracción del costo, aprovechando componentes comerciales (COTS) para una escalabilidad rápida y compatibilidad soberana.

Conclusión: Estados Unidos no puede superar en gasto ni en tiempo de espera a los adversarios cuánticos—pero sí puede superarlos en innovación.

Factor	Tipo Convencional 1	Isidore Quantum®
Campo de Tiempo	Horas/Días	Minutos
Costo por Nodo	$50K+	<$700
Consumo de Energía	35–50W	3W – 10W
Suministro de Hardware	Restringido	100% COTS (Listo para usar)
TRL / Validación	TRL 9 (No es a prueba de ataques cuánticos)	**TRL 8 (Resistencia Cuántica)**

Variantes y Especificaciones:

Isidore-1: IoT/OT/SCADA

Isidore 50MB/s – 2 GB/s

One-Way-Data Diode

CubeSat

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.					

1. Las especificaciones indicadas están sujetas a cambios sin previo aviso.

Contact: octans@inhub.world | forwardedge.ai | octanspace.com