White Paper

FORWARDEDGE

OCTANS SPACE AFRICA

Isidore Quantum®

Solución Integral de Ciberseguridad y PQC de Fácil Integración.

Listos para el Despegue: Cómo Proteger la Aviación de las Ciberamenazas Actuales y la Crisis Cuántica del Futuro.

¿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

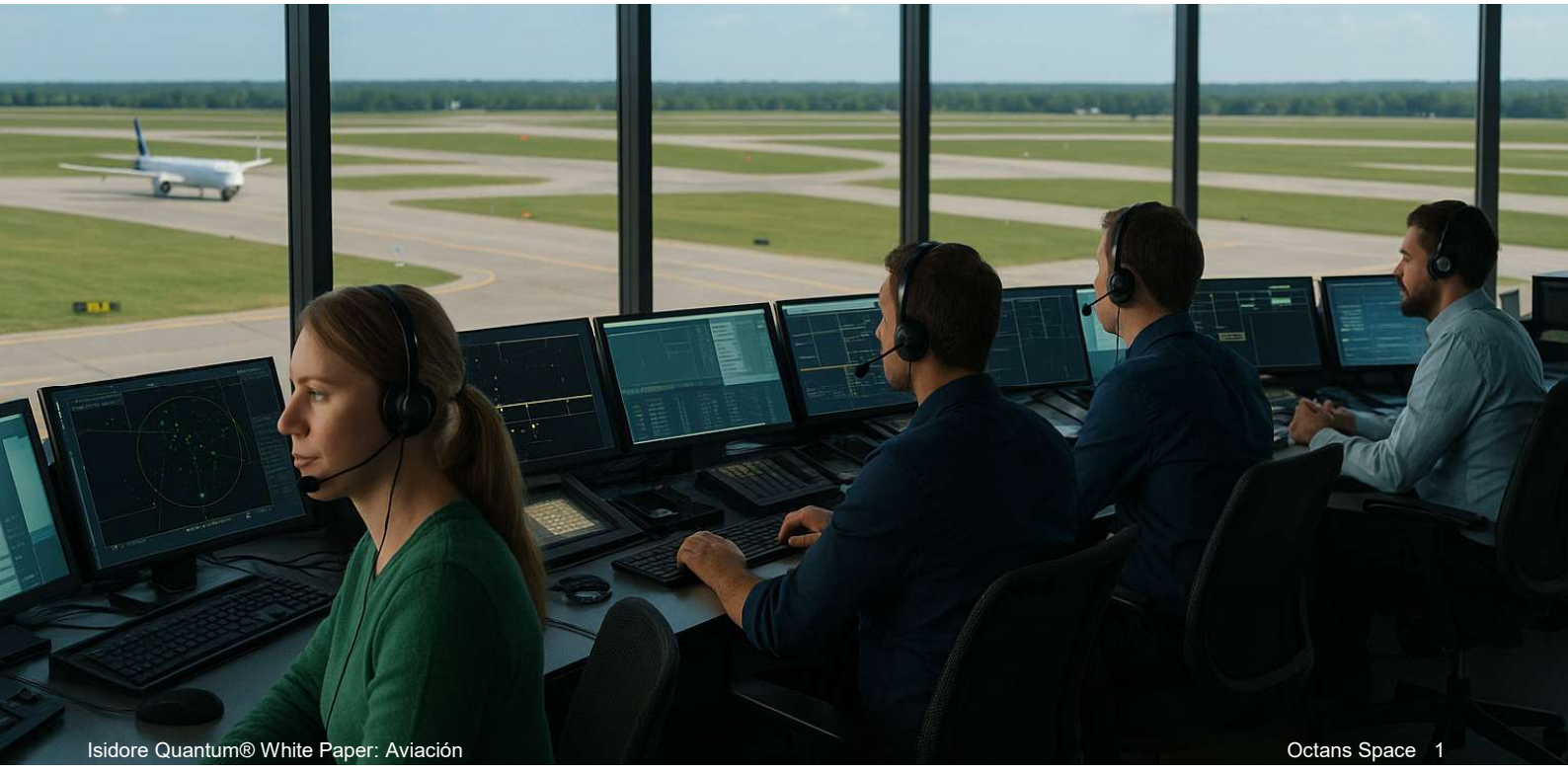
Ventaja Low-SWaP: Compacto, eficiente y escalable para uso en empresas, defensa e infraestructuras críticas.

La industria de la aviación enfrenta una crisis de ciberseguridad que se intensifica rápidamente, agravada por la emergente amenaza cuántica. Los sistemas modernos de control de tráfico aéreo, comunicaciones y datos, construidos sobre arquitecturas de décadas de antigüedad, ya están siendo objetivo de ransomware, intrusiones impulsadas por IA y ataques a la cadena de suministro que explotan protocolos no cifrados como ADS-B, CPDLC y SWIM. Las vulnerabilidades en estos sistemas exponen las operaciones de vuelo a suplantación, manipulación de datos y secuestro de comandos, incluso antes de que la computación cuántica alcance su plena capacidad ofensiva.

Los adversarios están llevando a cabo campañas de Harvest Now, Decrypt Later (HNDL), capturando hoy datos de aviación cifrados con la intención de descifrarlos cuando la tecnología cuántica sea capaz de romper los métodos de cifrado actuales. La creciente superposición entre ciberataques activos y la inminente amenaza de descifrado cuántico ha creado un nivel de riesgo sin precedentes para las redes globales de aviación.

Isidore Quantum, creado por Forward Edge-AI en colaboración con la NSA, proporciona una solución integral de ciberseguridad zero-trust poscuántica, diseñada para proteger los sistemas de aviación frente a ataques presentes y futuros. La plataforma integra detección de anomalías impulsada por IA, gestión autónoma de claves y cifrado compatible con CNSA 2.0 en un dispositivo de implementación directa (drop-in) que protege tanto redes heredadas como NextGen sin requerir costosas renovaciones de sistemas. El resultado es una vía práctica y resiliente de defensa para la industria aeronáutica en una era de amenazas digitales y cuánticas en aceleración.

El Q-Day no es un mito. Es una cuenta regresiva. La pregunta que enfrenta la aviación no es si ocurrirá la disrupción cuántica, sino si estaremos preparados.



La Amenaza para la Aviación

Por qué importa:

- ADS-B transmite sin cifrado: cualquiera puede suplantar posiciones de aeronaves o inyectar vuelos fantasma.
- CPDLC carece de autenticación: radios SDR de bajo costo pueden secuestrar enlaces de datos entre controlador y piloto.
- SWIM y SATCOM dependen de TLS y PKI: ambos colapsan ante ataques cuánticos.
- PKI heredada = punto único de falla sistémica: certificados, cargadores de claves y provisión manual no resisten la escala ni la velocidad.

La próxima crisis de la aviación comenzará en la red, no en los cielos. Los adversarios cibernéticos ya están infiltrando sistemas de vuelo, robando datos y preparándose para el momento en que las computadoras cuánticas vuelvan inútil el cifrado actual. Cuando ese punto llegue, cada señal no protegida se convertirá en un arma, y cada ruta de vuelo será un objetivo potencial. La amenaza ya ha llegado.

Sin protección poscuántica, las operaciones del espacio aéreo, el mantenimiento de flotas y la seguridad de los pasajeros enfrentan una exposición catastrófica. Solo el 17 % de las aerolíneas ha comenzado evaluaciones poscuánticas.

El Error de Percepción:

Los CISO retrasan la migración cuántica porque creen que la amenaza es “futura”. Sin embargo, los estados-nación ya están recolectando datos hoy, y el Q-Day podría llegar tan pronto como en 2026. Retrasar la acción garantiza la exposición retroactiva de décadas de datos de vuelo y canales de control.

Isidore Quantum: Solución Integral de Ciberseguridad Poscuántica (PQC)

Isidore Quantum es una plataforma compacta de ciberseguridad y cifrado poscuántico, desarrollada con ingeniería de la NSA y diseñada específicamente para proteger las comunicaciones y sistemas de control en la aviación. Diseñada para una integración directa (drop-in) y sin fricciones en redes ADS-B, CPDLC, SWIM y SATCOM, proporciona protección zero-trust conforme a CNSA 2.0 sin necesidad de rediseñar la infraestructura.
El dispositivo combina detección de amenazas impulsada por IA, gestión autónoma de claves y cifrado resistente a la computación cuántica para defenderse tanto de intrusiones cibernéticas actuales como de futuros ataques de descifrado cuántico. Ligero, eficiente energéticamente y validado en campo, Isidore Quantum garantiza una operación continua y segura en entornos de aviación comercial, defensa y control de tráfico aéreo a nivel mundial

Capacidades	Qué Significa
Arquitectura sin PKI	Elimina por completo certificados, firmas y la logística de cargadores de claves.
Cumplimiento CNSA 2.0	Utiliza AES-256-GCM y ML-KEM para el intercambio de claves poscuántico.
Antifragilidad Impulsada por IA	Aprende patrones de amenazas → detecta, aísla y se autorrecupera.
Aislamiento Rojo/Negro y Entropía Cuántica	Segmentación impuesta por hardware + generación de ruido aleatorio cuántico para claves únicas y verdaderamente aleatorias
Integración Plug-and-Play	Compatible con ARINC 429/653/664, MIL-STD-1553, Ethernet, Wi-Fi y SATCOM.
Factor de forma Low-SWaP (Borde)	< 8 W de consumo, tamaño de tarjeta de crédito, latencia inferior a milisegundos y rendimiento de 58 GB/s.

Por qué Importa:

- ADS-B transmite sin cifrado: cualquiera puede suplantar posiciones de aeronaves o inyectar vuelos fantasma.
- CPDLC carece de autenticación: radios SDR de bajo costo pueden secuestrar enlaces entre piloto y controlador.
- SWIM y SATCOM dependen de TLS y PKI: ambos colapsan ante ataques cuánticos.

Adaptación Operativa para la Aviación:

- Implementación directa (drop-in) en aviónica existente, routers ATC y redes aeroportuarias.
- Ciclo de vida de claves autónomo: sin provisión manual ni infraestructura de gestión de claves.
- Canales seguros en tiempo real resistentes a lo cuántico para ADS-B, CPDLC, SWIM y SATCOM.
- Motor ciberinmune basado en IA que aísla señales suplantadas y renueva claves en menos de 3 segundos.
- Cumple con los mandatos FAA NextGen e ICAO CyAP para protección zero-trust basada en datos.

Confiar únicamente en AES-256 crea una peligrosa ilusión de seguridad. El cifrado en sí 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 aferren a 'AES-256 es suficiente' corren el riesgo de proteger una bóveda vacía mientras los intrusos entran por puertas invisibles. La nueva era exige más que resistencia por fuerza bruta; exige arquitecturas diseñadas para resistir la velocidad cuántica, las fugas físicas y adversarios con inteligencia artificial.

Qué Deben Hacer Los Líderes Ahora

1. Auditar la Exposición del Cifrado - Identificar todos los sistemas que aún utilizan RSA, ECC o Diffie-Hellman.
2. Planificar la Transición a PQC - Alinear con los plazos de FAA NextGen e ICAO CyAP y sustituir PKI de forma temprana..
3. Implementar Isidore Quantum® - Comenzar por los canales de mayor riesgo: ADS-B, CPDLC, SATCOM y SWIM.
4. Colaborar y Compartir - Participar en pilotos industriales de Forward Edge-AI para validación entre redes.
5. Liderar, No Quedarse Atrás - El cumplimiento será pronto obligatorio (CNSA 2.0 para 2026). Los primeros en moverse definirán el estándar de seguridad poscuántica en la aviación.

Conclusión

El riesgo cuántico es inmediato. Isidore Quantum ofrece a los líderes de la aviación un escudo zero-trust, probado en campo y diseñado con estándares de la NSA: el único dispositivo PQC de implementación directa capaz de proteger tanto sistemas heredados como de próxima generación.

Cuando cada dólar, vatio y gramo cuenta, Isidore Quantum es la elección clara.

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