FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum® - 1 (Dispositivo de Borde)

Solución Integral de Ciberseguridad y Criptografía Poscuántica.

Garantizando la Seguridad de la Red: Defendiendo la Infraestructura Pública frente al colapso Cibernético y Cuántico.

¿Por qué Isidore Quantum?

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

Seguridad Resistente a la Computación Cuántica: protege los datos logísticos inalámbricos contra las amenazas de descifrado cuántico presentes y futuras.

Eficiencia de Bajo Consumo Energético (SWaP): Módulo compacto, ligero y de menos de 5W, ideal para vehículos, drones y dispositivos periféricos.

Defensa Impulsada por IA: predice, detecta y mitiga las ciberamenazas en tiempo real en todas las redes de la flota.

La infraestructura pública y los servicios esenciales, incluyendo la energía eléctrica, el gas natural, el agua, el alcantarillado, las telecomunicaciones, el ferrocarril y el transporte, están enfrentando ataques cada vez más intensos por parte de adversarios cibernéticos que explotan sistemas heredados que nunca fueron diseñados para las amenazas modernas. Las redes críticas dependen de dispositivos SCADA, PLC e IoT construidos para la fiabilidad más que para la resiliencia, lo que los deja expuestos a ransomware, explotación de acceso remoto y movimientos laterales a través de tecnologías operativas interconectadas. A medida que los atacantes se centran cada vez más en dependencias compartidas de OT, un solo punto comprometido puede desencadenar fallos en cascada que amenazan la seguridad nacional y la seguridad pública.

La cuenta regresiva hacia el Q-Day continúa, marcando el momento en que las computadoras cuánticas romperán la encriptación que protege todos los sistemas de control y harán obsoletos RSA, ECC y PKI. Los actores estatales ya están ejecutando campañas de “Harvest Now, Decrypt Later” (HNDL / Cosecha Ahora, Descifra Después), capturando hoy datos de infraestructura cifrados para su futura descodificación y uso como arma. La convergencia de las intrusiones cibernéticas en curso y la inminente amenaza de descifrado cuántico ha creado una tormenta perfecta capaz de socavar la confianza digital que sostiene los servicios más vitales del mundo.

Isidore Quantum, desarrollado por Forward Edge-AI en colaboración con la Agencia de Seguridad Nacional, proporciona una plataforma integral de ciberseguridad y cifrado post-cuántico diseñada para proteger la infraestructura crítica frente a amenazas actuales y emergentes. El sistema integra una arquitectura de confianza cero, gestión autónoma de claves y detección de anomalías impulsada por inteligencia artificial para asegurar redes SCADA, PLC y de telemetría en redes eléctricas, gasoductos, servicios de agua y sistemas de transporte, sin requerir costosas modernizaciones.

Totalmente compatible con CNSA 2.0 y equipado con algoritmos de cifrado resistentes a la computación cuántica, Isidore Quantum elimina las dependencias de PKI y los cargadores de claves obsoletos, ofreciendo protección en tiempo real y con capacidad de autorrecuperación en cada nodo de la red. Probado en implementaciones con la NSA, la Fuerza Aérea de los EE.UU. y la Marina de los EE.UU., la plataforma ofrece una resiliencia y escalabilidad inigualables. Los operadores de infraestructura adquieren la capacidad de reforzar sus defensas contra los ciberataques actuales, al tiempo que garantizan operaciones continuas y seguras frente a la computación cuántica durante las próximas décadas.

La Situación

56%	70%	US$5.6M	60%
Operadores SCADA/ICS informaron una violación en 2025	Las empresas de agua potable y saneamiento utilizan cifrado obsoleto y redes OT no segmentadas.	Coste promedio por incidente de ciberseguridad en el sector energético.	Los operadores de transporte han sufrido intentos o intrusiones cibernéticas.

Los sistemas de energía, agua, gas natural y transporte conforman la infraestructura invisible que sostiene la vida moderna, y todos están bajo ataque. Cada servicio público importante funciona actualmente dentro de un ecosistema digital hiperconectado de dispositivos SCADA, PLC e IoT diseñados para la fiabilidad más que para la ciberseguridad. Los sistemas heredados, muchos de los cuales aún operan con firmware de décadas de antigüedad, son cada vez más objeto de ataques mediante ransomware, explotación de acceso remoto y manipulación de datos.

Estos eventos no son aislados, sino que reflejan un marco de seguridad en colapso, basado en la confianza y en sistemas de cifrado que no pueden resistir la llegada de la era cuántica.

Isidore Quantum: Solución integral de ciberseguridad PQC

Isidore Quantum es una plataforma compacta de ciberseguridad y cifrado post-cuántico, desarrollada por la NSA, diseñada para proteger infraestructuras críticas —incluyendo energía eléctrica, gas natural, agua, alcantarillado, telecomunicaciones, ferrocarriles y sistemas de transporte— frente a amenazas cibernéticas tanto actuales como emergentes.
La plataforma ofrece protección de confianza cero, compatible con CNSA 2.0, mediante gestión autónoma de claves y detección de anomalías impulsada por inteligencia artificial, capaz de identificar y aislar intrusiones de forma inmediata. Diseñada para integrarse sin problemas con redes SCADA, PLC y OT heredadas, Isidore Quantum elimina las dependencias de PKI y se instala sin necesidad de costosas modificaciones de infraestructura.
Probado tanto en entornos de defensa como en servicios públicos comerciales, el sistema proporciona una solución unificada y escalable que fortalece los servicios esenciales frente a los ciberataques actuales, al tiempo que los prepara para los futuros desafíos de descifrado cuántico.

Capacidad	Lo Que Ofrece
Cifrado Resistente a la Computación Cuántica	Reemplaza RSA/ECC con ML-KEM y AES-256-GCM, asegurando el tráfico de SCADA, PLC y telemetría frente a ataques tanto cuánticos como clásicos
Confianza Cero por Defecto	Aplica emparejamiento criptográfico entre cada punto final: ningún dispositivo ni usuario es confiable por defecto
Inmunidad a Amenazas Impulsada por IA	Detecta y aísla anomalías en redes de energía, agua y ferrocarril en tiempo real, reduciendo el tiempo medio de respuesta de horas a segundos
Ciclo de Vida Autónomo de Claves	Genera y renueva automáticamente claves de sesión efímeras, eliminando PKI, cargadores de claves y ciclos de renovación de certificados
Aislamiento Rojo/Negro y Entropía Cuántica	Segmentación reforzada por hardware junto con generación de ruido cuántico aleatorio para claves de un solo uso demostrablemente aleatorias
Integración Plug-and-Play (Conectar y Usar)	Se implementa en minutos sobre Ethernet, SATCOM, fibra o radio, sin tiempo de inactividad ni necesidad de rediseñar el sistema

Confiar únicamente en AES-256 crea una peligrosa ilusión de seguridad. El cifrado en sí sigue siendo sólido, pero la estructura que lo rodea ya se está desmoronando. Los algoritmos cuánticos atravesarán 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.
Los defensores que 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 se avecina exige más que resistencia a la fuerza bruta; exige arquitecturas diseñadas para resistir la velocidad cuántica, las filtraciones físicas y los adversarios con inteligencia artificial.

La Urgencia para Infraestructura Pública

Retrasar la migración hacia la criptografía post-cuántica abre la puerta a fallos en cascada en los sistemas de energía, agua y transporte. Como han dejado claro la NSA, el NIST y el DHS, los sistemas que no se modernicen antes de 2027 dejarán de cumplir con los estándares de seguridad nacional y regulatorios.

Actúe ahora para:

1. Auditar las dependencias de cifrado OT—identificar exposición a RSA, ECC y PKI.
2. Desplegar Isidore Quantum® en gateways SCADA (pasarelas), subestaciones y nodos de control.
3. Adoptar arquitecturas de confianza cero compatibles con PQC para cumplir con los mandatos CNSA 2.0.
4. Proteger sus datos ahora—antes de que los adversarios los descifren en el futuro.

Conclusión

Los servicios públicos son la base de la civilización—y el próximo frente de la guerra cibernética. Isidore Quantum® es la primera y única plataforma de ciberseguridad resiliente a la computación cuántica, lista para integrarse ("drop-in"), probada en sistemas de defensa, energía, agua y transporte.

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