

CASO 26 - Implementación de soluciones cuántico-seguras en comunicaciones OT de una planta de generación de recursos energéticos

Consorcio: Ayesa Ibermatica; i3B

Tecnología: Ciberseguridad; Digital trust

Descripción general:

El sector energético y, en particular, el refino de petróleo, combina procesos continuos, activos de alto valor, sistemas de control distribuidos, comunicaciones OT en tiempo real y requisitos estrictos de seguridad industrial. Una refinería como Petronor en Muskiz integra unidades de proceso, utilities, tanques, bombeos, cargaderos, redes industriales, sistemas SCADA/DCS, sensórica crítica, comunicaciones inalámbricas en campo y accesos de mantenimiento.

La digitalización industrial y el uso creciente de robots, AGV, sensórica inalámbrica, mantenimiento remoto y analítica de operación incrementan la superficie de exposición. Aunque muchas comunicaciones actuales pueden estar cifradas frente a ataques clásicos, los algoritmos de clave pública más extendidos, como RSA y ECC, están expuestos a la evolución futura de la computación cuántica. Además, la amenaza de tipo harvest now, decrypt later permite capturar hoy tráfico cifrado y descifrarlo cuando exista capacidad cuántica suficiente.

El caso se particulariza para una infraestructura energética de alta criticidad operativa: la refinería de Petronor en Muskiz. La solución propuesta consiste en diseñar, desplegar y validar una arquitectura de comunicaciones OT cuántico-seguras para flujos inalámbricos y de borde industrial, con especial atención, sensórica IIoT, gateways OT, SCADA/DCS y accesos de gestión remoto

El objetivo de la actuación es preparar la transición de las comunicaciones industriales críticas hacia criptografía resistente a ataques cuánticos, reduciendo el riesgo de interceptación, exfiltración, suplantación de dispositivos, manipulación de telemetría e inyección de órdenes fraudulentas. La justificación principal no es únicamente tecnológica: en un entorno de refino, una comunicación OT alterada puede afectar a la continuidad operativa, a la seguridad industrial, a la integridad de los procesos y a la protección de información sensible sobre operación de planta.

Programa: Red.es

Duración: 8 meses (01/05/2026 – 31/12/2026)

Presupuesto global proyecto: 80.000,00€

Presupuesto Grupo Ayesa: 80.000,00 €

red.es



Unión Europea

Fondo Europeo
de Desarrollo Regional
"Una manera de hacer Europa"



**Plan de Recuperación,
Transformación
y Resiliencia**

Financiado por la Unión Europea – Next Generation EU –

CASO 26 - Implementación de soluciones cuántico-seguras en comunicaciones OT de una planta de generación de recursos energéticos

Consorcio: Ayesa Ibermatica; i3B

Tecnología: Ciberseguridad; Digital trust

Rol de Ayesa:

Ayesa líder del caso de uso será la entidad responsable de la coordinación técnica y operativa en ciberseguridad OT, criptografía post-cuántica, integración industrial y validación de comunicaciones, en el entorno energético en colaboración con Petronor como entorno industrial de referencia.

La propuesta se plantea como una prueba de concepto de transición PQC para infraestructuras energéticas críticas. El despliegue se realizará de forma progresiva, no intrusiva y medible, empezando por gateways y flujos representativos antes de intervenir PLC, DCS o lazos de control críticos. El piloto validará esquemas híbridos clásico + post-cuántico, perfiles criptoágiles y mecanismos de firma de órdenes críticas, manteniendo requisitos industriales de disponibilidad, latencia y trazabilidad.

