

**PREGUNTAS DE LICITADORES RECIBIDAS AL 30 DE MAYO DEL 2025  
DE LA CONVOCATORIA DE LICITACIÓN DEL CONTRATO DE  
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO QKD Y  
ENCRİPTADORES PARA EL PROYECTO MADQUANTUM-CM  
A ADJUDICAR POR PROCEDIMIENTO ABIERTO CON PLURALIDAD DE  
CRITERIOS.  
EXP. QKD-MADQCI.**

**PREGUNTA 1.**

*“¿Pueden indicarnos una estimación del número de enlaces físicos (o bien número de puertos) por equipo y tipo de cifrador (IPsec y MACsec) que serán desplegados? O bien, en su defecto, una estimación del número global de enlaces que se estima desplegar para cada tipo de cifrador (IPsec y MACsec).”*

**RESPUESTA 1.**

No se establece un número concreto de puertos que deban ser proporcionados. La definición de esta cantidad queda bajo la responsabilidad del integrador, quien deberá determinarla en función del diseño técnico que proponga. Será, por tanto, el integrador quien, en base a su conocimiento, experiencia y criterios técnicos, deberá dimensionar adecuadamente la solución para asegurar que se cumplen todos los requisitos establecidos en el punto 3.2 del pliego, así como lo descrito en la solución técnica recogida en el punto 4. Este enfoque otorga flexibilidad al integrador para plantear la arquitectura más adecuada, siempre garantizando el cumplimiento de las especificaciones funcionales, operativas y de rendimiento exigidas por el proyecto.

**PREGUNTA 2.**

*“En relación con la licitación correspondiente al expediente QKD-MADQCI, les escribimos para solicitar una aclaración específica sobre la posibilidad de subcontratar el soporte de Nivel 1 y Nivel 2.*

*En el Pliego de Cláusulas Administrativas, apartado 20, se indica que:*

*“Prestaciones no susceptibles de subcontratación: el soporte de nivel 3 debe prestarse por el fabricante.”*

*“Indicación en la oferta de la parte del contrato que se pretenda subcontratar: Sí”*

*A partir de esta información, entendemos que la subcontratación del soporte de Nivel 1 y Nivel 2 sería posible, siempre que se indique correctamente en la oferta.*

*No obstante, en el Pliego de Prescripciones Técnicas se indica que:*

*“Todas las necesidades y prestaciones que se requieren para la garantía especificada en este apartado deben ser proporcionadas **directamente** por el adjudicatario del contrato.”*

*Dado que esta redacción puede dar lugar a interpretaciones distintas, necesitamos confirmar expresamente si el adjudicatario puede subcontratar total*

*o parcialmente el soporte de Nivel 1 y Nivel 2, cumpliendo en todo caso con los requisitos técnicos exigidos en el pliego.”*

## **RESPUESTA 2.**

La sección de mantenimiento está organizada según el tipo de equipamiento. En el caso de los equipos QKD, no se establece que el soporte de nivel 1 (N1) y nivel 2 (N2) deba ser prestado directamente por el adjudicatario del contrato. Por tanto, este servicio puede ser subcontratado a un tercero, siempre que se respeten los estándares de calidad y los tiempos de respuesta definidos. En el caso de los equipos encriptadores, aunque inicialmente se indicaba que el soporte debía ser prestado directamente por el adjudicatario, se ha detectado una errata. Al igual que con los equipos QKD, tanto el soporte de nivel 1 como el de nivel 2 podrá ser subcontratado, siempre que se garanticen los niveles de calidad y los tiempos de respuesta establecidos.

## **PREGUNTA 3.**

*“A continuación, encontrará nuestras preguntas aclaratorias:*

*1. Doble fuente de alimentación:*

*¿Se refiere a que el dispositivo debe ser compatible con la conexión a dos fuentes de alimentación independientes en el centro de datos o a otra cosa?*

*2. Requisito de entropía de QRNG:*

*¿Es la especificación de 1 Mbps de entropía cuántica real un requisito estricto para QRNG?*

*3. Canal de posprocesamiento:*

*¿Podría confirmar si el canal de servicio (posprocesamiento) y el canal cuántico pueden compartir la misma fibra física o si es obligatoria una conexión RJ45 independiente?*

*4. Alcance del soporte adicional (20 puntos):*

*Agradeceríamos cualquier aclaración sobre el alcance de los servicios de soporte adicionales mencionados.*

*Específicamente:*

- ¿El soporte solicitado después del primer año incluye aspectos logísticos como el envío desde/hacia las instalaciones?*

- ¿Se prevé también la provisión de un sistema de reemplazo durante el mantenimiento o una falla del equipo?*

*5. Cumplimiento de los estándares ETSI y SKIP:*

*¿Debe el sistema cumplir con los tres estándares (ETSI GS QKD 014, ETSI GS QKD 004 y SKIP), o es suficiente con cumplir con al menos uno de ellos?*

*6. KMS – Copia de seguridad y recuperación de claves:*

*¿Podría proporcionar más detalles sobre el significado de "copia de seguridad y recuperación de claves sin comprometer su confidencialidad ni integridad"?*

*7. Sección 3.1.3 – Inventario y servicios:*

*En relación con ""*

*Estas interfaces abiertas basadas en estándares deben permitir la consulta y extracción de información como:*

*Inventario*

*Números de serie*

*Servicios*

*Información de topología de red*

*""*

- *¿Qué información específica se espera en "Inventario" y "Servicios"?"*

### **RESPUESTA 3.**

- 1) Rreferido al equipamiento QKD: tal como se indica en los requisitos, **solo si se solicita**, los equipos deben contar con doble fuente de alimentación. La forma en la que estas fuentes se conecten puede variar en función de las características específicas de cada CPD.
- 2) Todos los requisitos indicados en el pliego tienen carácter obligatorio, salvo que se indique expresamente lo contrario mediante términos como "recomendable" u otros sinónimos que impliquen no obligatoriedad.
- 3) Como en la pregunta anterior, no queda claro si te estás refiriendo a QKD-CV o a QKD-DV. En cualquier caso, si revisas los requisitos, verás que se contemplan varias opciones de conexión. Aunque se indica una configuración ideal, se permiten otras alternativas que también se consideran válidas dentro de los parámetros establecidos.
- 4) El mantenimiento, tanto durante el periodo obligatorio como en el caso de que se oferte una ampliación, debe ser el mismo en cuanto a alcance y condiciones. Esto está claramente especificado en el punto 6 del PPT, donde se detalla que se requiere soporte en los niveles N1, N2 y N3.

Por tanto, el mantenimiento solicitado incluye no solo los aspectos mencionados en tu pregunta, sino también todo lo que se indica expresamente en dicho apartado del PPT, abarcando todas las necesidades operativas, de soporte y de resolución de incidencias definidas para el servicio.

- 5) Con que cumpla un estandar es suficiente.
- 6) Cuando el pliego exige "mecanismos de respaldo y recuperación de claves sin comprometer su confidencialidad o integridad", en el contexto de un sistema QKD (Quantum Key Distribution), se solicita que el sistema disponga de procesos que garanticen que las claves generadas puedan ser respaldadas y recuperadas en caso de fallo operativo o de red, sin que esto implique ningún riesgo de exposición o alteración de las mismas.

Este requisito está alineado con las recomendaciones de seguridad definidas por ETSI (por ejemplo, en ETSI GS QKD 015 y ETSI GS QKD

004), donde se establece que cualquier mecanismo adicional que gestione claves derivadas de QKD debe mantener el mismo nivel de seguridad criptográfica que el canal cuántico original.

7) Esto dependerá de cada fabricante, pero en general esperamos:

### **Inventario**

La información de inventario esperada debería incluir tanto elementos físicos como lógicos del sistema QKD. Específicamente:

- Equipamiento QKD físico:
  - o Tipo y modelo del sistema QKD (DV, CV, etc.).
  - o Fabricante y número de serie.
  - o Estado del equipo (activo, en standby, fuera de servicio).
  - o Versión de firmware/software.
  - o Puertos de comunicación utilizados (clásico y cuántico).
  - o Ubicación física del nodo.
- Módulos auxiliares:
  - o Sistemas de cifrado asociados, si forman parte de la solución integrada.
  - o Estado de las fuentes de alimentación redundantes, ventilación, etc.

### **Servicios**

Aquí se refiere a los servicios criptográficos o de red habilitados sobre la infraestructura QKD. Por ejemplo:

- Sesiones de distribución de claves:
  - o Estado actual de la sesión (activa, fallida, en negociación).
  - o Volumen de claves generadas y tasa de generación (kbps o similar).
  - o Tipo de protocolo QKD utilizado (BB84, CV-QKD, etc.).
  - o Parámetros de calidad: tasa de error cuántico (QBER), visibilidad, etc.
- Integración con sistemas de cifrado clásicos:
  - o Servicios de sincronización de claves con cifradores.
  - o Política de renovación de claves (frecuencia, mecanismos).
  - o Logs de uso o fallos en el intercambio.

En general, el objetivo de estas interfaces es proporcionar visibilidad completa sobre el estado operativo del sistema QKD y su uso real en la red, facilitando tanto la monitorización como la interoperabilidad con plataformas externas.

## **PREGUNTA 4.**

***Discrepancia en el criterio de valoración “Mejora en la capacidad de MACsec”***  
*En la página 8 del PCAP se indica:*

*"Se exige un cifrado y descifrado MACsec a velocidad de línea de hasta 2 Gb/s por puerto. Se otorgarán 2,5 puntos adicionales por cada incremento de 2 Gb/s sobre el mínimo requerido."*

*Sin embargo, el apartado 3.2.2 del PPT establece:*

*"El dispositivo debería proporcionar cifrado y descifrado MACsec a velocidad de línea de hasta 12 Gb/s en puertos de tipo SFP28 y hasta 10 Gb/s en puertos para ópticas de tipo SFP+, añadiendo una latencia máxima de 2 microsegundos."*

*¿Podrían aclarar cuál debe considerarse como base para la puntuación en este criterio objetivo: los 2 Gb/s del PCAP o las velocidades mayores descritas en el PPT?*

#### **RESPUESTA 4.**

En este caso, la interpretación correcta es la que figura en el PPT. En el PCAP hay una errata tipográfica: falta un "1" delante del "2", por lo que la velocidad mínima requerida debería ser de 12 Gb/s para puertos SFP28 y de 10 Gb/s para SFP+, tal como se detalla en el PPT.

#### **PREGUNTA 5.**

***Discrepancia en el criterio de valoración "Mejora en la capacidad de IPsec"***  
*En el PCAP, página 8:*

*"Se exige un throughput agregado igual o superior a 3 Gb/s. Se otorgarán 2,5 puntos adicionales por cada incremento de 2 Gb/s sobre el mínimo requerido."*

*Sin embargo, en el PPT, apartado 3.2.1, se detalla:*

*"El dispositivo deberá permitir al menos 100 túneles IPsec concurrentes con un throughput agregado  $\geq 2,5$  Gb/s y latencia añadida  $\geq 40$  microsegundos para paquetes de 64 bytes."*

*¿Nos podrían confirmar cuál es el throughput mínimo exigido en este caso: 3 Gb/s como indica el PCAP, o 2,5 Gb/s según el PPT? Asimismo, ¿la mejora valorable (incrementos de 2,5 Gb/s) debe mantenerse siempre bajo la condición de los 100 túneles concurrentes?*

#### **RESPUESTA 5.**

La información correcta es la que aparece en el PPT: el throughput mínimo exigido es  $\geq 2,5$  Gb/s. El valor de 3 Gb/s mencionado en el PCAP es erróneo. Además, la condición de los 100 túneles IPsec concurrentes se mantiene como requisito para la evaluación de cualquier mejora en este criterio.

#### **PREGUNTA 6.**

**Aclaración sobre la acreditación de la solvencia técnica**

*En el PCAP, página 6, se indica:*

*"... siendo el requisito mínimo que el importe anual acumulado en el año de mayor ejecución sea igual o superior al 70% del valor estimado del contrato, o de su anualidad media si esta es inferior al valor estimado del contrato."*

*No queda clara la interpretación de la frase "o de su anualidad media si esta es inferior al valor estimado del contrato".*

*¿Podrían ofrecernos un ejemplo práctico que permita comprender mejor este criterio?*

**RESPUESTA 6.**

Lo que se tiene que acreditar es que o el importe anual de uno de los últimos 3 años es el 70% del valor estimado del contrato, o que la media de los tres años es al menos el 70% de dicho valor estimado.

Pozuelo de Alarcón, 10 de junio del 2025.