PLIEGO DE CLÁUSULAS TÉCNICAS QUE HAN DE REGIR LA CONTRATACIÓN DE SUMINISTRO DE EQUIPOS, SOPORTE, ASISTENCIA TÉCNICA Y FORMACIÓN PARA PILOTO DE DISTRIBUCIÓN CUÁNTICA DE CLAVES (QKD)

Febrero 2026/2026ko otsaila

Navarra de Servicios y Tecnologías, S.A.
| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |
| info@nasertic.es | www.nasertic.es
| Tel: 848 420 500 | Fax: 848 426 751

ÍNDICE

1. Contexto general

La distribución cuántica de claves (QKD, Quantum Key Distribution) surge del solapamiento de tres campos bien diferenciados: las comunicaciones, la seguridad y la física cuántica. Pese a que los artículos seminales se remontan a finales del pasado siglo (BB84, E91), el interés por QKD se ha multiplicado recientemente, en especial a causa de los avances en computación cuántica y el subsiguiente riesgo de rotura de protocolos de encriptación tradicionalmente confiables tales como RSA y AES. Hay diversos factores que condicionan el análisis de este riesgo en seguridad. Uno de los ellos, —quizás el principal— reside en estimar el plazo en el cual se producirá un acceso generalizado a los sistemas de computación cuántica, el cual podría poner a disposición de grupos de usuarios malintencionados herramientas para ejecutar algoritmos que permitan desencriptar las comunicaciones actuales. Por desgracia, no hay unanimidad acerca de cuándo puede llegar este punto de inflexión. Algunas predicciones muy optimistas hablan de que en 5 años podrían empezar a estar disponibles los primeros computadores cuánticos en entornos de producción, mientras que otras predicciones más conservadoras retrasan el uso generalizado de esta tecnología hasta dentro de 20 años.

Siendo la amenaza en seguridad no inmediata, ¿cuál es el interés de proteger nuestros sistemas de encriptación desde ya? La principal razón es el denominado *harvest now decrypt latter*. Este término recoge la idea de que es posible capturar tráfico con información sensible ahora para explotarlo en el futuro cuando la tecnología lo permita. Esta circunstancia, unida al hecho de que determinados datos (datos personales, de salud o de hacienda pública, entre otros) no son de carácter fungible, sino que pueden seguir siendo válidos y sensibles durante muchos años, hace que administraciones públicas, empresas y operadores de telecomunicaciones deban ponerse manos a la obra para mejorar los mecanismos de encriptación actuales. QKD es una de las tecnologías destinadas a auxiliarnos en la resolución este problema.

¿Por qué QKD?

Hoy en día, la seguridad en encriptación en comunicaciones de datos se apoya, fundamentalmente, en dos protocolos bastante antiguos que fueron impulsados en Estados Unidos por el MIT (Massachusetts Institute of Technology) y el NIST (National Institute of Standards and Technology) en 1971 y 2001, respectivamente: RSA y AES. La encriptación RSA

(Rivest-Shamir-Adleman) es asimétrica, esto es, usa una clave para encriptar y otra para desencriptar, y se basa en el problema de factorizar números enteros grandes en números primos. La encriptación AES (Advanced Encryption Standard) es simétrica, esto es, usa la misma clave para encriptar y desencriptar, se basa en el algoritmo Rijndael y se considera irrompible mediante tecnologías de computación tradicionales para claves de 256 bits (AES-256). Estos dos protocolos son básicos para la securización de la mayoría de los sistemas de comunicaciones actuales. RSA, por ejemplo, juega un papel fundamental en el funcionamiento de los certificados SSL/TLS que se usan en la comunicación HTTPS y en la firma digital, que es una de las piezas claves de la administración electrónica. AES, por su parte, también se emplea en los protocolos SSL/TLS y, en combinación con WAP2, securiza muchas de las conexiones WIFI actuales. En definitiva, no exclusivamente, pero sí fundamentalmente, RSA y AES son los pilares sobre los que se apoya la privacidad, integridad y autenticidad de las comunicaciones que hoy en día se cursan por las redes públicas.

Aunque todavía sean considerados confiables, estos protocolos de encriptación tradicionales se enfrentan a dos grandes problemas: la interceptación de claves públicas durante su transmisión a través de canales no seguros y los ataques basados en fuerza bruta. Estos dos problemas requieren una solución de compromiso. Cuanta mayor es la rotación de claves, más resistente es el sistema ante ataques de fuerza bruta, ya que estos necesitan disponer de muestras de información relativamente grandes para poder ser exitosos. Paradójicamente, cuanto mayor es la rotación de claves, más necesaria es la transmisión de claves por canales no seguros, lo que incrementa el riesgo de interceptación.

La irrupción de la computación cuántica unida a algoritmia ha vuelto a poner el foco de atención en estos problemas y amenaza con romper la resistencia de los protocolos tradicionales tales como RSA y AES. En concreto, el algoritmo de Shor (1994) es capaz de factorizar números enteros grandes de manera eficiente y amenaza con romper la encriptación RSA. Por otro lado, el algoritmo de Grover (1996) facilita la realización de ataques de fuerza bruta en sistemas basados en encriptación simétrica tales como AES. En un futuro no muy lejano, la combinación de estos y otros algoritmos unidos a la velocidad de computación de los ordenadores cuánticos hará posible romper en cuestión de horas mecanismos de encriptación que hoy en día son virtualmente irrompibles.

Ante esta amenaza existen, en la actualidad, dos estrategias de mitigación bien diferenciadas y complementarias: PQC (Post-Quantum Cryptography) y QKD (Quantum Key Distribution).

PQC mantiene la estrategia de defenderse de los ataques de algoritmia a través de más algoritmia, y se basa en el desarrollo de nuevos problemas complejos que no sean rompibles a través de computación cuántica (es decir, que sean *quantum safe*). Por su parte, QKD se enfrenta a los nuevos retos de seguridad a través de la capa física, y está basado en el uso de propiedades y principios propios de la física cuántica para securizar la distribución de claves y poder aumentar, de ese modo, la frecuencia de rotación de estas de manera segura.

La tecnología QKD resuelve de manera novedosa al menos dos problemas:

- Resuelve el problema de la distribución de claves. En QKD no hay distribución de clave a través del canal de datos, ni a través de ningún canal. Por el contrario, los sistemas son capaces de crear claves aleatorias en dos puntos distantes entre ellos mediante el uso de propiedades físicas de fotones o haces de luz, haciendo uso de los principios fundamentales de la física cuántica tales como el entrelazamiento, la superposición y el principio de incertidumbre. QKD se puede usar para aumentar de manera segura la rotación de claves e impedir los ataques de fuerza bruta.
- Resuelve el problema de la detección de intrusiones en el canal cuántico, ya que el problema de la medida hace que cualquier intrusión (que, al fin y al cabo, no es sino una medida) afecte las medidas subsiguientes. Mediante la supervisión de muestras aleatorias de medición cuántica, los sistemas QKD son capaces de detectar que existe intrusión y tomar medidas adecuadas.

QKD es una tecnología en ciernes, pero rupturista, que dispone de equipos en el mercado y por la que ya apuestan decididamente países como Japón y China. En Europa existe también un impulso importante en favor del QKD terrestre y del QKD aéreo, el cual se plasma en programas tales como EuroQCI -2027 y EAGLE-1 2026. Usada por separado o en combinación con otros mecanismos de criptografía postcuántica, la tecnología QKD será seguramente un factor clave en la securización de las redes futuras.

¿Por qué NavCC y Nasertic?

El Navarra Cybersecurity Center (NavCC) es centro de referencia en materia de ciberseguridad en Navarra, siendo su principal objetivo el impulso al desarrollo de iniciativas en torno a la ciberseguridad que generen un aumento de la ciber resiliencia en todos los ámbitos de la Comunidad Foral de Navarra: ciudadanía, tejido empresarial, talento y administraciones

públicas. En esencia, busca que la sociedad navarra esté mejor preparada para enfrentar a un posible ciberataque, y para ello pone el foco en las tres "C's" de la ciberseguridad: concienciación, cultura y capacidades.

El Navarra Cybersecurity Center (NavCC) es una iniciativa liderada por el Departamento de Universidad, Innovación y Transformación Digital del Gobierno de Navarra, y gestionada por la Sociedad Pública NASERTIC, enmarcada en el proyecto colaborativo CIBERREG - *Impulso a la ciberseguridad desde los territorios* -, que cuenta con la participación de otras siete regiones españolas y que forma parte del programa RETECH (Redes Territoriales de Especialización Tecnológica), impulsado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, coordinado por INCIBE y financiado con fondos del Plan de Recuperación, Transformación y Resiliencia (Next Generation).

Entre las iniciativas que promueve el NavCC se cuenta la labor de divulgación y concienciación acerca de las amenazas en ciberseguridad. En este sentido, Navarra no es ajena a la problemática generalizada que se deriva del uso de sistemas de encriptación tradicionales tales como RSA y AES en el ámbito de la salud, la educación, la industria o la administración electrónica. El proyecto de implantación de un piloto de QKD aplicado a una red de transporte permitirá evaluar y probar esta tecnología en equipos reales. El piloto, además, podrá ser puesto a disposición del público en talleres prácticos abiertos en los cuales se puedan, no sólo profundizar en la problemática actual de la seguridad en las comunicaciones, sino también realizar demostraciones prácticas del funcionamiento de la tecnología en un escenario real.

Por su parte, Nasertic es una empresa pública del Gobierno de Navarra, parte de Corporación Pública Empresarial de Navarra (CPEN). Entre su ámbito de actuación se encuentra la promoción de nuevas tecnologías en el ámbito de la modernización y el desarrollo de la Comunidad Foral de Navarra. Nasertic es operador de red, y gestiona diferentes redes de transporte de la Comunidad Foral de Navarra. Como operador, una de las responsabilidades de Nasertic es la de velar por la seguridad de las comunicaciones transportadas por las redes que gestiona. En este sentido, el proyecto de QKD es un impulso para evaluar la tecnología de encriptación y elaborar un plan de protección del tráfico en la capa de transporte, esto es, de manera específica e independientemente de la existencia de otros mecanismos de encriptación de la información implementados en niveles superiores.

2. Objeto

NavCC y Nasertic desean disponer de un piloto compuesto de dos equipos QKD, los cuales se integrarán con una pareja de equipos de transporte propiedad de Nasertic para la encriptación del tráfico de transporte mediante protocolos tales como MACSec o similar. Este piloto consistirá en la instalación, puesta en marcha y evaluación de la funcionalidad de los equipos y la tecnología QKD en un escenario de red de transporte real entre dos sedes corporativas. En particular, se analizará el comportamiento de la tecnología en las siguientes situaciones:

- Funcionamiento de encriptación MACSec entre dos equipos de transporte que consuman parejas de claves distribuidas cuánticamente.
- Rendimiento de la solución de encriptación en situación de rotación frecuente de clave.
- Comportamiento y resiliencia del sistema en un escenario de intrusión del canal óptico. Evaluación de la resistencia del sistema de encriptación en este caso y de la sensibilidad del equipo para la detección de la intrusión.
- Nivel de disponibilidad de la solución en caso de fallo del sistema de distribución de claves.

En cuanto al aspecto divulgativo, el proyecto permitirá disponer de un piloto de QKD que se pueda poner a disposición de terceros para pruebas y que pueda ser empleado para realizar talleres de divulgación, concienciación y acercamiento de tecnologías relacionadas con la seguridad en la Comunidad Foral de Navarra.

Dentro de ese contexto se enmarca la presente licitación. El objeto de esta es el **suministro de una pareja de equipos QKD con soporte para 2 años**, así como los servicios para **la asistencia técnica** de configuración de esos equipos en un entorno de pruebas definido por NavCC/Nasertic y los **servicios de formación** acerca de la tecnología en general y los equipos en particular.

Los equipos serán instalados por Nasertic en el entorno de pruebas y se integrarán con equipos de transporte propios para su uso en la securización de comunicaciones existentes.

Por consiguiente, quedan excluidos de esta licitación los trabajos de instalación física de los equipos QKD, así como el suministro de equipos de encriptación adicionales.

3. Descripción de productos requeridos

La presente licitación incluye los siguientes productos.

3.1. Suministro de equipos QKD

Se solicita el suministro de una pareja de equipos de QKD compuesta de transmisor y receptor y completamente equipados para generación de pares de claves distribuidas cuánticamente en conexiones punto a punto realizadas mediante fibra monomodo. También se suministrará un sistema de gestión de claves para mitigación de problemas en caso de intrusión en el canal de distribución de claves.

3.2. Soporte técnico para equipos QKD

Además, se solicita servicios de soporte técnico para los dos equipos QKD durante al menos 2 años.

3.3. Asistencia técnica en piloto

Se solicitan servicios de asistencia técnica que incluirán la participación en la configuración e integración de los equipos QKD suministrados con equipos de comunicaciones existentes en dos escenarios PaP (punto a punto):

1. Asistencia para la configuración y pruebas de los QKD en el entorno de laboratorio, en configuración punto a punto, teniendo en cuenta que Nasertic realizará la instalación de todos los equipos y la configuración de los equipos de comunicaciones

consumidores de las claves. Por consiguiente, la asistencia incluirá el diseño de la solución, la configuración de los equipos QKD, así como el apoyo para integración con los equipos de comunicaciones.

2. Asistencia para la configuración y pruebas de los QKD en el entorno de servicio para la conexión de una sede concreta, en configuración punto a punto, siempre en un enlace de menos de 40 km, teniendo en cuenta que Nasertic realizará la instalación de todos los equipos y la configuración de los equipos de comunicaciones consumidores de las claves. Por consiguiente, la asistencia incluirá el diseño de la solución, la configuración de los equipos QKD, así como el apoyo para integración con los equipos de comunicaciones.

Para la realización de estos dos escenarios NavCC/Nasertic pondrá a disposición equipos de comunicaciones propios. Las pruebas se realizarán con los siguientes equipos:

- 2 x Juniper ACX 7024, compatibles con MACSec.

Los transceptores disponibles para las pruebas con objeto de realizar la conexión entre los equipos de comunicaciones son los siguientes:

- Transceptores Juniper SFP-25G-BX40D-I & SFP-25G-BX40U-I, que emplean una única fibra óptica y operan en los rangos de longitud de onda 1260-1280 nm y 1300 -1320 nm.

3.4. Formación tecnológica

Teniendo en cuenta los objetivos del proyecto y su carácter de innovación tecnológica, se otorga gran importancia al aspecto formativo de la licitación. Para ello, se solicitan servicios de formación tecnológica que abarquen los siguientes aspectos:

- Estado del arte actual de la tecnología, en los campos de computación cuántica, comunicaciones cuánticas y sensórica cuántica.
- Estado del arte actual de la tecnología cuántica aplicada a comunicaciones, con especial atención a criptografía, situación y riesgos actuales.
- Quantum Key Distribution en sus distintas versiones, incluyendo análisis pormenorizado de sus fortalezas y debilidades.

- Protocolos de distribución de claves clásicos y cuánticos.
- Casos de uso actuales de la QKD.
- Funcionamiento interno de los equipos de compartición de claves.
- Criptografía postcuántica y su relación con la QKD.

Los servicios de formación se compondrán de dos tipos de formación:

- Formación de un mínimo de dos jornadas (de 8h cada una de ellas) para el personal de NavCC/Nasertic (10 asistentes) acerca de los aspectos antes indicados.
- Impartición de tres talleres prácticos abiertos a público por determinar, cada uno de ellos de 4h de duración que incluya formación acerca de tecnologías cuánticas, QKD y demostración práctica del funcionamiento del piloto que se haya instalado.

4. Prescripciones técnicas

En los siguientes apartados se relacionan las prescripciones técnicas particulares que obligatoriamente habrán de cumplir los equipos, así como de aquellas otras características que tendrán peso en la valoración técnica de las ofertas.

Las siguientes prescripciones técnicas serán de carácter obligatorio, siempre de acuerdo con los criterios detallados en el presente pliego.

Las especificaciones técnicas de obligado cumplimiento recibirán un código de este tipo:

OBLx

donde:

- x es el índice incremental de la especificación y tomará valores 1, 2, 3…
- **OBL** indica que el requerimiento es obligatorio.

Cada licitador deberá presentar cumplimentada en formato electrónico la tabla del **Anexo I Plantilla requisitos obligatorios**, indicando el cumplimiento de su oferta con los requisitos detallados.

Por su parte, las especificaciones técnicas valorables se indicarán mediante el uso del siguiente código:

VTECx

donde:

- x es el índice incremental de la especificación y tomará valores 1, 2, 3, etc.
- **VTEC** indica que el requerimiento es valorable técnico (criterio cualitativo).

Tanto la puntuación de cada aspecto valorable, como las fórmulas de valoración subjetiva quedan recogidas en el **Anexo II – Puntuación de aspectos técnicos valorables**.

Por último, habrá aspectos valorables con carácter objetivo, los cuales se valorarán de acuerdo con criterios objetivos sin incluir especificaciones técnicas. Es importante resaltar que la memoria técnica presentada por los participantes en la licitación no debe hacer ninguna referencia a estos aspectos valorables objetivos, puesto que serán objeto de valoración junto con la valoración económica.

Los criterios valorables de carácter objetivo recibirán el siguiente código:

VOBJx

donde:

- x es el índice incremental de la especificación y tomará valores 1, 2, 3, etc.
- **VOBJ** indica que el requerimiento es valorable objetivo (criterio cuantitativo).

Tanto la puntuación de cada aspecto valorable, como las fórmulas de valoración quedan recogidas en el pliego de condiciones administrativas.

Aquellas ofertas que no cumplan las especificaciones obligatorias indicadas en este apartado de prescripciones técnicas particulares serán objeto de exclusión del procedimiento de licitación.

Igualmente será motivo de exclusión la falta de justificación adecuada del cumplimiento de los requerimientos obligatorios solicitados. Para ello, el licitador deberá presentar una breve memoria técnica de justificación de cumplimiento de requerimientos técnicos obligatorios y valorables.

4.1. Requerimientos del equipamiento QKD

A continuación, se presentan los requerimientos tecnológicos de los equipos.

OBL1 El material incluido en este suministro no debe estar incluido en procesos de discontinuidad, descatalogación o fin de vida del fabricante.

OBL2 El suministro debe incluir todas las licencias necesarias para el correcto funcionamiento y cumplimiento de los requerimientos obligatorios de este pliego.

OBL3 Cada uno de los equipos QKD deberá ser enracable en rack de 19 pulgadas, ocupando un tamaño máximo de 3RU. Si fuera necesario instalar algún equipamiento adicional para la realización correcta de las pruebas de piloto, estos equipos serán preferentemente enracables y, en cualquier caso, su tamaño no deberá ocupar más de 3RU adicionales.

OBL4 Los equipos QKD suministrados deben ser capaces de generar pares de clave secreta en ambos extremos de una conexión punto a punto, utilizando para ello propiedades de la mecánica cuántica, y protocolos de distribución cuántica de claves QKD, esto es, que no estén basados en el envío específico de la clave de cifrado. En particular, no se aceptarán soluciones basadas en la transmisión cifrada de claves, o que estén esencialmente basadas en criptografía postcuántica, incluso aunque sean consideradas “quantum safe”. Por el contrario, se

aceptarán soluciones que estén esencialmente basadas en protocolos QKD tales como BB84, E91, u otras soluciones QKD tanto de variable discreta como de variable continua, incluso aunque estas se apoyen, de manera auxiliar, en criptografía postcuántica.

OBL5 Los equipos QKD suministrados deben ser suficientes para poder realizar las pruebas piloto indicadas en este pliego de condiciones técnicas. En otras palabras, deben poder integrarse directamente con los equipos de transporte propiedad de Nasertic en la configuración punto a punto. En caso de que la solución requiera de algún elemento adicional para realizar esa integración, este elemento deberá ser incluido en el suministro sin coste adicional a lo licitado en este pliego.

VTEC1 Se valorará las referencias de casos de uso de la tecnología ofertada. En particular, se valorará que se presenten hasta dos referencias contratables. Se considerará referencia contrastable aquella que tenga un alto grado de similitud con respecto al caso descrito en este pliego, especialmente si está relacionado con el uso de QKD en entornos de operador de telecomunicaciones, en el ámbito de la administración pública y/o con integración con equipos de transporte similares o asimilables a los descritos en el pliego. Se valorará también la presentación de otras referencias adicionales.

OBL6 Los equipos QKD deben ser capaces de generar claves cuánticas mediante uso de una única fibra óptica monomodo dedicada para ello. Para ello, deberán venir equipados con los transmisores y receptores ópticos correspondientes.

VTEC2 Se valorará que la solución permita usar para la distribución de claves cuánticas la misma fibra de comunicaciones que se emplea como canal, mediante el uso de bandas específicas y mecanismos de multiplexación. Para la valoración de este aspecto se tendrá en cuenta cuál es la frecuencia empleada en la solución con fibra no dedicada, así como su compatibilidad con usos de comunicaciones en DWMD y CWDM sin degradación significativa del rendimiento. También se valorará que en la oferta se incluya el suministro de los componentes adicionales (mux/demux) para la realización de pruebas en el entorno de piloto en esa situación de compartición de canal. A tal efecto, en el apartado 3.3 se indican los rangos de longitud de onda en los que operarán los transceptores empleados para conectar los equipos de comunicación.

OBL7 Los equipos QKD deben ser capaces de generar claves cuánticas de manera estable en enlaces de fibra óptica de mínimo 40 km. NOTA: se toma como referencia una pérdida de 0,3 dB/km, en la cual se incluyen pérdidas de conectores, fusiones, elementos pasivos intermedios y pérdidas de transmisión. En total, por tanto, los equipos deberán funcionar correctamente y de manera estable en enlaces ópticos con una pérdida total de 12 dB entre transmisor y receptor.

OBL8 Los equipos QKD deberán ser capaces de generar claves como mínimo a una tasa de generación de 500 b/s (bits por segundo).

OBL9 Los equipos QKD deben venir equipados con puerto de 1 Gbps para la entrega de claves y con puerto ethernet de cobre para gestión de red.

OBL10 Los equipos QKD debe ser gestionables mediante interface cli (ssh v2) y/o web (http/https). Asimismo, también deben permitir la gestión mediante snmp (v2 o v3). El suministrador deberá entregar el árbol MIB para facilitar la integración en la plataforma de gestión de red de Nasertic.

OBL11 El acceso de usuarios a los equipos QKD debe ser contabilizado y registrado, para permitir tener históricos de acceso.

VTEC3 Se valorará la tecnología utilizada para la distribución de claves cuánticas. Para la valoración de este punto, los licitadores deberán incluir información acerca del tipo de tecnología usada (variable discreta, variable continua y, dentro de cada tipo, el mecanismo o tecnología particular), incluyendo documentación de fabricante o referencias bibliográficas de la solución. En particular, se valorará tanto el grado de detalle en la descripción de la tecnología, así como el grado de adecuación de esta tecnología al caso de uso particular descrito en este pliego.

OBL12 Los equipos QKD deben venir provistos de algún tipo de mecanismo de mitigación frente a situación de intrusión en el canal óptico que implique la imposibilidad de generar

nuevas claves durante un cierto periodo de tiempo. Las ofertas deberán explicar en qué consisten estos mecanismos de mitigación. En particular, la oferta deberá incluir sistema de gestión de claves (KMS), bien sea externo, bien sea incluido en los dos equipos QKD.

VTEC4 Se valorarán los mecanismos de mitigación frente a situación de intrusión. En particular, se valorará el sistema de gestión de claves de claves KMS, siempre y cuando esta solución permita mitigar la situación de intrusión en el canal óptico. Además, se valorará también el grado de adecuación de la solución ofertada al caso de uso particular descrito en este pliego, esto es, consistente en dos sedes separadas por 20km.

4.2. Requerimientos del soporte técnico del equipamiento

A continuación, se presentan los requerimientos tecnológicos para el soporte de nivel 2 de los equipos suministrados

OBL13 Además de la pareja de equipos QKD la solución debe incluir servicio de soporte de fabricante para 2 años. Este servicio de soporte debe incluir los siguientes aspectos:

- Acceso a últimas versiones de software de los equipos.
- Atención a incidencias relacionadas con aspectos funcionales de los equipos.
- Sustitución de equipos o sus componentes en caso de avería.

VOBJ1 Se valorará positivamente que la oferta contemple la ampliación del soporte, hasta dos años por encima de lo exigido en pliego. SE RECUERDA QUE LA MEMORIA TÉCNICA y DOCUMENTACIÓN INCLUIDA EN EL SOBRE 1 NO DEBE HACER REFERENCIA EXPLÍCITA A CRITERIOS VALORABLES OBJETIVOS, YA QUE ESTOS SERÁN VALORADOS JUNTO CON LA OFERTA ECONÓMICA EN EL SOBRE 2.

OBL14 El soporte del equipamiento deberán cumplir los acuerdos de servicio descritos en este pliego.

Acuerdo de nivel de servicio

El nivel de servicio que Nasertic tiene comprometido con sus clientes se mide mediante un conjunto de parámetros, que se han determinado como los más adecuados, en cada una de las facetas de la provisión y el aseguramiento de los servicios de telecomunicaciones.

En los apartados siguientes se definen expresamente los parámetros de nivel de servicio para que después puedan ser aplicados de manera correcta y sin ambigüedad.

Parámetros de aseguramiento del servicio

Con el fin de utilizar el mismo criterio a la hora de definir cualquier parámetro para el aseguramiento del servicio, se describen a continuación los más importantes.

- **Incidente**: se considera un incidente todo aquel evento no programado que causa o puede llegar a causar una pérdida en la calidad del servicio.
- **Tiempo de respuesta**: tiempo máximo, contado a partir de la notificación del aviso o incidencia correspondiente por parte de Nasertic a la empresa adjudicataria hasta el momento en que el técnico asignado por la empresa adjudicataria para la resolución de dicho incidente se pone en contacto con Nasertic para proceder al diagnóstico de esta. En este tiempo, Nasertic deberá conocer los datos de la persona que se va a encargar de gestionar la resolución de la avería, nombre y teléfono de contacto, y así deberá reflejarse en la herramienta correspondiente.
- **Tiempo de presencia in situ**: tiempo transcurrido desde la notificación del aviso o incidencia correspondiente por parte de Nasertic a la empresa adjudicataria hasta el inicio in situ de las actividades de diagnóstico y/o reparación a realizar in situ en el punto de la red en el que se ha detectado el incidente, incluido el desplazamiento de los técnicos de la empresa adjudicataria hasta dicha localización equipados con los materiales, maquinaria y medios auxiliares necesarios para su resolución. Este tiempo aplica únicamente a las actuaciones relacionadas con la asistencia de los servicios NPN en frecuencia de operador.
- **Tiempo de resolución:** tiempo transcurrido desde que se recibe el incidente hasta que se restaura el servicio afectado, ya sea mediante una solución definitiva o cualquier solución alternativa que permita la continuidad del servicio. Este valor es acumulativo para una única actuación y representa el tiempo neto total de la actividad destinado

por parte de la empresa adjudicataria a la ejecución de la actuación, una vez descontados los tiempos de parada.

- **Tiempo de parada:** Es el tiempo consumido por actividades realizadas por terceros o por aquellas circunstancias que no permitan la actuación de manera temporal y directa de la empresa adjudicataria sobre la actuación demandada y que por lo tanto han provocado una "parada de reloj". Este valor es acumulativo tantas veces como se produzca la "parada de reloj" durante la resolución de una actuación. Los tiempos de parada no serán efectivos en el cálculo del total del tiempo de resolución de la incidencia por parte de la empresa adjudicataria. Las paradas de reloj por parte del adjudicatario deben estar justificadas, adecuadamente documentadas y con el visto bueno de NASERTIC.
- **Prioridad del incidente**: La prioridad de los incidentes se establece en base a los conceptos de urgencia e impacto, que se clasificarán en función de los siguientes criterios: tipo de sede (crítica, principal o secundaria), tipo de servicio (esencial o no esencial) y tipo de afección (caída total, degradación y sin afección). Atendiendo a su urgencia e impacto, se definen cuatro tipos de prioridades (de 1 a 4, correspondiendo el 1 a la máxima prioridad y el 4 a la mínima) que podrán tener distintos tiempos de resolución.

IMPACTO	descripción
crítico	Afección a todos los servicios NPN en todas las ubicaciones
alto	Afección a los servicios en dos o más ubicaciones
normal	Afección sólo en una ubicación

Tabla 1

URGENCIA	descripción
crítica	Caída total de servicio esencial
alta	Degradación de un servicio esencial o caída de un servicio no esencial
normal	Degradación de un servicio no esencial o sin afección de servicio

Tabla 2

La siguiente tabla resume las prioridades que aplican a los distintos incidentes.

IMPACTO	crítico	alto	normal
URGENCIA			
crítica	prioridad 1	prioridad 2	prioridad 3
alta	prioridad 2	prioridad 3	prioridad 3
normal	prioridad 3	prioridad 3	prioridad 4

Tabla 3

Horario de recepción de incidencias y actuación

El horario de recepción de avisos, por cualquiera de los canales establecidos, y de actuación será de 12x5 (lunes a viernes).

Compromisos de resolución (ANS)

Los compromisos de resolución de incidencias apuntalan los acuerdos de nivel de servicio prestados por el equipamiento de las redes de transporte.

Los tiempos objetivo para tratamiento de incidentes dependen de la prioridad asignada a los mismos, y son los indicados en la Tabla 4.

PRIORIDAD	Tiempo de respuesta	Tiempo de resolución
Prioridad 1	15 minutos	5 horas
Prioridad 2	15 minutos	10 horas
Prioridad 3	15 minutos	24 horas
Prioridad 4	15 minutos	7 días

Tabla 4

Los tiempos objetivo para tratamiento de consultas dependen de la prioridad asignada a los mismos, y son los indicados en la Tabla 5.

PRIORIDAD	Tiempo de respuesta	Tiempo de resolución
Prioridad 1	4 horas	24 horas
Prioridad 2	8 horas	3 días
Prioridad 3	24 horas	7 días
Prioridad 4	24 horas	7 días

Tabla 5

4.3. Requerimientos de la asistencia técnica en el piloto

A continuación, se presentan los requerimientos de la asistencia técnica en los dos escenarios.

OBL15 Se requiere asistencia técnica para los dos escenarios indicados en este pliego de condiciones técnicas, a saber, escenario PaP de laboratorio y escenario real PaP de conexión de una sede con enlace óptico de menos de 40 km. El objetivo en ambos escenarios es probar la encriptación MACSec, y verificar la estabilidad, disponibilidad y funcionalidad de la solución para garantizar confidencialidad, integridad y autenticidad mediante el uso de la tecnología QKD.

OBL16 El licitador deberá presentar una propuesta de batería de pruebas que incluya los siguientes aspectos:

- Funcionamiento de encriptación MACSec entre los dos equipos de transporte en la situación de consumo de parejas de claves distribuidas cuánticamente.
- Rendimiento de la solución de encriptación en situación de rotación frecuente de clave.

- Comportamiento y resiliencia del sistema en un escenario de intrusión del canal óptico. Evaluación de la resistencia del sistema de encriptación en este caso y de la sensibilidad del equipo para la detección de la intrusión.
- Comportamiento y resiliencia de la solución en caso de fallo del sistema de distribución de claves.

VTEC5 Se valorará la propuesta de batería de pruebas con los equipos. En particular, se valorará el grado de detalle del plan (desglose, descripción de pruebas, objetivos y definición de procedimientos) así como el nivel de adecuación y particularización del plan al caso de uso descrito en este pliego.

VTEC6 Se valorará positivamente que el licitador ponga a disposición de NavCC/Nasertic durante el periodo de pruebas un equipo de intrusión de señal óptica con el cual se puedan realizar las pruebas de funcionamiento del sistema. Este equipo se valorará de acuerdo con sus especificaciones técnicas y nivel funcional. Si no fuera posible disponer del interceptador, se valorará positivamente que la propuesta incluya un procedimiento para simular la intrusión de manera manual. Este procedimiento se valorará de acuerdo con el detalle de su descripción, así como de acuerdo con el grado de adecuación de la solución al caso de uso descrito en este pliego.

4.4. Requerimientos de formación

OBL17 Se solicita un temario de formación para el personal de NavCC/Nasertic de mínimo 2 jornadas (8h cada jornada) cuyo contenido incluirá aspectos de la tecnología en general y del piloto QKD implementado en particular.

OBL18 Se solicita que el temario sea diseñado sin presuponer conocimientos previos en tecnologías cuánticas ni en criptografía. Por otro lado, este temario no deberá estar focalizado exclusivamente en el equipo y la tecnología proporcionada por el licitador. Los licitadores deberán incluir un plan de formación cuyo contenido incluya los siguientes aspectos:

- Parte 1, más generalista, enfocada a las tecnologías cuánticas aplicadas a la seguridad y a QKD, explicando las diferentes posibilidades.
- Parte 2, más particular del equipamiento ofertado, enfocada a conocer tanto la tecnología de distribución cuántica de claves como al piloto realizado.

VTEC7 Se valorará el contenido del temario de formación. En particular, se valorará el grado de descripción y detalle del temario propuesto, la flexibilidad y adaptabilidad del temario. También se valorará el nivel de adecuación del temario al caso de uso descrito en este pliego. Por último, de valorará el nivel de adecuación, experiencia formadora y formación académica de la persona encargada de impartir la formación. Para ello, los licitadores deberán incluir información académica relevante acerca de la persona que hará la formación. SE RECUERDA QUE AL DESCRIBIR EL CONTENIDO DEL TEMARIO NO SE DEBE INCLUIR NINGUNA REFERENCIA A LA PLANIFICACIÓN EN FECHAS, Y EN CONCRETO AL NÚMERO DE JORNADAS DE LA FORMACIÓN, YA QUE ESTE ES UN CRITERIO VALORABLE OBJETIVO QUE ÚNICAMENTE DEBE IR EN EL SOBRE 2).

VOBJ2 Se valorará positivamente que el licitador oferte un aumento de las jornadas de formación por encima de las exigidas en pliego, y siempre hasta un máximo de dos jornadas adicionales. SE RECUERDA QUE LA MEMORIA TÉCNICA y DOCUMENTACIÓN INCLUIDA EN EL SOBRE 1 NO DEBE HACER REFERENCIA EXPLÍCITA A CRITERIOS VALORABLES OBJETIVOS, YA QUE ESTOS SERÁN VALORADOS JUNTO CON LA OFERTA ECONÓMICA EN EL SOBRE 2.

OBL19 Se solicita la impartición de tres talleres divulgativos, dedicados al público del ámbito académico, consistentes cada uno de ellos de 4 horas, acerca de la tecnología y el piloto QKD. Los tres talleres podrán tener un contenido similar, puesto que cada uno de ellos estará dirigido a diferentes públicos. Los talleres se impartirán en fechas a determinar por NavCC/Nasertic, y siempre durante 2026. Los licitadores deberán incluir un plan de contenidos para los talleres que, en cualquier caso, deberá incluir los siguientes aspectos:

- Formación generalista acerca de las tecnologías cuánticas relacionadas con la seguridad.
- Presentación práctica del funcionamiento con uso de los equipos QKD instalados en piloto.

VTEC8 Se valorará el contenido del plan de impartición del taller. En particular, se valorará el grado de descripción y detalle del temario propuesto, la flexibilidad y adaptabilidad del plan. También se valorará el nivel de adecuación de la formación al caso de uso descrito en este pliego. Por último, de valorará el nivel de adecuación, experiencia formadora y formación académica de la persona encargada de impartir la formación. Para ello, los licitadores deberán incluir información académica relevante acerca de la persona que hará la formación. SE RECUERDA QUE AL DESCRIBIR EL PLAN DE IMPLANTACIÓN NO SE DEBE HACER REFERENCIA EXPLÍCITA AL NÚMERO DE JORNADAS DE IMPARTICIÓN DEL TALLER, YA QUE ESTE ES UN CRITERIO OBJETIVO QUE ÚNICAMENTE DEBE IR EN EL SOBRE 2.

VOBJ3 Se valorará que el licitador ofrezca jornadas adicionales de impartición del taller por encima de las exigidas en pliego hasta un máximo de dos jornadas adicionales. La impartición de estas jornadas adicionales se realizará en las mismas condiciones que el taller inicial exigido en pliego y con un contenido similar. SE RECUERDA QUE LA MEMORIA TÉCNICA y DOCUMENTACIÓN INCLUIDA EN EL SOBRE 1 NO DEBE HACER REFERENCIA EXPLÍCITA A CRITERIOS VALORABLES OBJETIVOS, YA QUE ESTOS SERÁN VALORADOS JUNTO CON LA OFERTA ECONÓMICA EN EL SOBRE 2.

OBL20 Tanto la formación como los talleres se realizarán de manera presencial, en ubicaciones por determinar, siempre en Navarra.

5. Requerimientos en suministro

Los requerimientos de este apartado se refieren al suministro de los materiales objeto de licitación.

El suministro de materiales objeto del presente procedimiento deberá realizarse de arreglo a las siguientes fases:

1. NavCC/Nasertic dará el visto bueno a los materiales antes de tramitar el pedido siguiendo los criterios indicados en Pliego de Condiciones Regulatorias de esta licitación.

2. NavCC/Nasertic confirmará el lugar de entrega del material.
3. A la entrega del pedido, NavCC/Nasertic procederá al inventario del material en el punto de entrega.
4. Una vez comprobado el inventario, se procederá a la firma del acta de recepción definitiva.

OBL21 El licitador se compromete a informar del estado del pedido cumplimentando los siguientes hitos referenciados a las siguientes fechas:

- Pedido recibido y tramitado a fabricante.
- Fecha prevista de fabricación (si aplica).
- Fecha prevista de salida de almacén o de fábrica.
- Fecha prevista de entrega en almacén de NavCC/Nasertic.

OBL22 El licitador se compromete a entregar los dos equipos QKD antes del 31 de mayo de 2026.

OBL23 El licitador se compromete a que, en caso de resultar adjudicatario, la factura que se emita una vez realizados los trabajos tenga un desglose que permita distinguir claramente y sin ambigüedad los cuatro ítems de esta contratación, a saber, suministro de equipos, soporte técnico, asistencia técnica y formación, todo ello a efectos de la posterior justificación de fondos.