Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informació

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE RIGE LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN Y PUESTA EN PRODUCCIÓN DE EQUIPAMIENTOS DE DISTRIBUCIÓN DE CLAVE CUÁNTICA

Expediente nº: CTTI-2026-36

Finançat per la Unió Europea

1. OBJETO

El objeto de la presente licitación es el suministro, instalación y puesta en producción de equipamientos de distribución de claves cuánticas (QKD), con sistema de gestión de claves (KMS) y generador cuántico de números aleatorios (QRNG), integrado en la red de conectividad de la Generalitat de Catalunya.

En concreto, el objeto del contrato incluye las fases siguientes:

- Fase 1. Plan de migración: Elaboración de un plan para migrar, de una red óptica compleja, a una red óptica con seguridad post-cuántica. Categorización y priorización de nodos, definición de requerimientos.

- Fase 2. Ejecución crítica: Suministro, instalación, configuración y puesta en producción de los equipamientos en sedes y segmentos críticos (en los nodos previstos a la fase inicial), creando un bloque de comunicaciones encriptado cuánticamente.

- Fase 3. Despliegue: Despliegue y ampliación del anterior bloque de comunicaciones encriptado en los nodos restantes previstos. Incluye, como en el punto anterior, el suministro e instalación física de equipos, configuración y puesta en producción.

- Fase 4. Análisis de los datos: Observación, análisis de datos y formación, que incluye principalmente: evaluación del comportamiento, monitorización, tráfico y extracción de conclusiones.

2. DESCRIPCIÓN DE LAS PRESTACIONES DE LAS FASES

El alcance de esta licitación contempla los siguientes servicios y suministros a realizar a cada fase:

- Fase Plan de migración
- Fase Ejecución crítica (suministros e instalación de la fase inicial)
- Fase Despliegue
- Fase Análisis de los datos

2.1. Fase Plan de migración

Esta fase consiste en la elaboración de un plan para migrar la actual red óptica hacia una red óptica con seguridad post-cuántica, así como el análisis, categorización y priorización de los nodos cuánticos y definición de requerimientos.

Este plan deberá incluir, al menos:

- Definición concreta de los objetivos:
    - Categorización de nodos. Identificación de distancias entre nodos, puntos críticos, segmentos relacionales entre ellos y tipo de tráfico con el fin de garantizar que la información cuántica viaje sin interrupciones.
    - Ubicación de nodos. Definición del alcance geográfico concreto, en Barcelona y su área metropolitana, con el fin de obtener resultados prácticos en redes reales.
    - Establecimiento de criterios de priorización de nodos y sedes. Se requiere nodos conectados con fibra óptica, con pérdidas que no superen el umbral máximo.
    - Análisis y definición de requerimientos. Análisis y definición de disponibilidad de espacios y otros requerimientos. Los nodos de red disponen de salas técnicas aptas para incluir los equipamientos requeridos.
    - Valoración de conclusiones. Valoración de viabilidad de la intervención. Entrega de un entregable final que recoja las conclusiones sobre el alcance del despliegue de equipamientos cuánticos.
- Descripción de la topología.
- Requisitos previos.
- Diseño final de la nueva arquitectura.
- Descripción de las dos siguientes fases (fase de ejecución crítica y fase despliegue):
    - Nodos de red y sedes implicadas.
    - Equipamiento que desplegar en cada nodo de red o sede.
    - Planificación detallada, con fechas y descripción de las actuaciones.
    - Planes de reversibilidad (rollback) para cada fase.

- Definición de pruebas y validación
    - Entre las pruebas a realizar, hará falta la prueba de integración para cada nodo QKD y KMS: Verificación de la generación, transmisión, recepción y uso correcto de las claves con los equipos de red del nodo. El proveedor tendrá que certificar el resultado, validado por los técnicos del CTTI.
- Evaluación de riesgos y medidas de mitigación.
- Descripción del cronograma y recursos asociados.
- Se definirá y acordará con el CTTI el contenido, y la periodicidad, de los informes operativos y ejecutivos, para el seguimiento y control de las tareas y fases del contrato. El CTTI se reserva el derecho de modificar los informes establecidos, solicitar nuevos informes periódicos o ad-hoc, e introducir cambios en cualquier momento de la vigencia del contrato según las necesidades del servicio.
- Acceso por parte de quien determine el CTTI a una herramienta de seguimiento de proyecto. Actualizada como mínimo de forma diaria, con el fin de garantizar un control continuado y alineado con los requerimientos establecidos a cada fase.

Gestión de los accesos de los técnicos a los nodos y sedes de la Generalitat tenidos en cuenta en el plan incluyendo la generación y actualización de la documentación necesaria de PRL en la herramienta de control de PRL / CAE.

2.2. Fase Ejecución crítica

Suministro e instalación de equipamiento en cuatro (4) de los doce nodos previstos en el plan de migración

Se puede tratar, por ejemplo, del segmento entre dos centros de procesamiento de datos, el ámbito del área metropolitana adyacente y los principales edificios dentro del segmento, creando así un bloque de comunicaciones encriptado cuánticamente.

Suministro e instalación física de equipos, ajuste de las configuraciones y puesta en producción. Esta prueba inicial tiene que permitir detectar posibles errores de planificación y obtener primeros datos de análisis.

El objetivo es integrar y validar la interconexión de todos los equipos necesarios en un entorno de laboratorio, para elevar la madurez de la tecnología a un TRL8 (sistema completo y certificado, con tecnología acabada, testada y validada formalmente para ser operativa y segura).

Eso se conseguirá llevando a cabo las primeras pruebas y puesta en marcha de la tecnología garantizando la interoperabilidad para su posterior despliegue en los nodos en producción.

Durante esta fase, es fundamental que los fabricantes de KMS, QKD y Generalitat colaboren de manera estrecha para garantizar que la solución integral cumpla con todos los requisitos identificados para el despliegue en entornos de producción.

Esta etapa permitirá definir con precisión los casos de uso, las aplicaciones y los servicios disponibles, así como los aspectos operativos esenciales, como la gestión y monitorización integral de la solución.

Las actividades mínimas a realizar serán:

- Suministro de los equipos necesarios para los primeros nodos.

- Despliegue inicial de los equipos. Instalación física de los equipos de los dos primeros nodos y configuración básica para la puesta en marcha de los mismos. Uno de estos dos nodos tendrá que corresponder obligatoriamente al nodo ubicado en el entorno de laboratorio, que tendrá que quedar plenamente operativo desde el despliegue inicial.
- Calibración y paso a producción. Ajuste de las configuraciones de los nuevos equipos y de los equipos existentes para garantizar la comunicación entre extremos y su correcta encriptación.
- Escalado del tercer nodo. Despliegue de los equipos del tercer nodo y evaluación del impacto al complicar la arquitectura de dos a tres nodos y puesta en producción.
- Escalado al resto de nodos. Despliegue del resto de nodos hasta completar los cuatro de esta fase. Evaluación de cómo se comporta esta arquitectura más compleja. Puesta en producción.
- En caso de que el CTTI decida poner en producción alguno de los nodos desplegados durante esta fase, el licitador tendrá que efectuar el traspaso técnico correspondiente al equipo designado por el CTTI, incluyendo la documentación, la configuración y cualquier otro elemento necesario para su correcta operación.
- La monitorización de los equipos puestos en marcha se tendrá que integrar con la monitorización del centro de control.
- Gestión del mantenimiento y garantía de los productos con el objetivo de garantizar la disponibilidad de los equipos puestos en producción.

2.3. Fase Despliegue

Despliegue y ampliación del bloque de comunicaciones encriptado cuánticamente a los 8 nodos restantes con el fin de obtener una red óptica protegida en un volumen que permita conseguir conclusiones válidas con respecto a instalación real, instalación operativa, integración en red real, operación y mantenimiento reales, métricas de impacto real, retrasos, eficiencia y consumos.

Asegurar la integración y validación de la interconexión de todos los equipos necesarios elevando la madurez de la tecnología, al menos, en un TRL8 (sistema completo y certificado, con tecnología acabada, testada y validada formalmente para ser operativa y segura).

Las actividades a realizar, como mínimo, serán:

- Suministro de los equipos. Suministro de los equipos necesarios para los nodos de esta fase.
- Escalado a cuatro nodos más. Despliegue de cuatro nodos adicionales en base a la experiencia de despliegue de los anteriores y evaluación de posibles incrementos temporales. Evaluación del comportamiento de esta nueva arquitectura, la cual cerraría el anillo metropolitano. Puesta en producción.
- Escalado final. Despliegue de los últimos cuatro nodos y sedes. Evaluación del comportamiento de esta nueva arquitectura, con varias sedes desplegadas conectadas a los nodos y en el anillo. Puesta en producción.
- Mantenimiento del entorno de laboratorio operativo y en ejecución. El entorno de laboratorio tendrá que mantenerse activo y plenamente operativo durante toda la vigencia del contrato, con capacidad para llevar a cabo tanto pruebas internas

como pruebas abiertas con terceros, según las necesidades del CTTI. Finalizado el contrato, el laboratorio no podrá ser desmontado ni retirado, y tendrá que quedar como infraestructura permanente del CTTI, a su disposición para futuras pruebas, validaciones y actividades de desarrollo relacionadas.

- En caso de que el CTTI decida poner en producción alguno de los nodos desplegados durante esta fase, el licitador tendrá que efectuar el traspaso técnico correspondiente al equipo designado por el CTTI, incluyendo la documentación, la configuración y cualquier otro elemento necesario para su correcta operación.

2.4. Fase Análisis de los datos

Observación y análisis de los datos en operación real durante un periodo de tiempo que permita extraer conclusiones relacionadas con el producto evolucionado en el mercado.

Las actividades principales necesarias para llevar a cabo la actuación serán:

- Análisis de datos del tráfico entre los dos primeros nodos. Evaluación del comportamiento del tráfico entre los dos primeros nodos encriptados.
- Análisis de datos del tráfico entre los cuatro primeros nodos. Evaluación del comportamiento y del tráfico entre los cuatro primeros nodos encriptados y el impacto de la complejidad de la nueva arquitectura.
- Análisis de datos del tráfico dentro del anillo metropolitano. Evaluación del comportamiento y del tráfico dentro de los nodos del anillo metropolitano encriptados y el impacto de la complejidad de la nueva arquitectura.
- Análisis de la red completa. Evaluación del comportamiento y del tráfico entre el anillo metropolitano y las sedes conectadas, distinguiendo topologías y peculiaridades de las señales transmitidas.
- Elaboración y entrega del documento que recoja, de manera estructurada y con detalle, los datos de observación, los análisis realizados y las conclusiones derivadas en esta fase.
- Formación y transferencia de conocimiento de los aspectos fundamentales de operación descrita en el apartado 5.5 Plan de devolución del servicio de este PPT.

3. CARACTERÍSTICAS DE LOS EQUIPOS A SUMINISTRAR

3.1. Equipamientos QKD (CV-QKD y QRNG)

Los sistemas de distribución cuántica de claves basados en variables continuas (CV-QKD) permiten la generación y transmisión segura de claves criptográficas mediante propiedades cuánticas de la luz, como la amplitud y la fase de campos electromagnéticos coherentes. Estas comunicaciones se basan en parejas de equipos formados por un emisor y un receptor, que interactúan a través de un canal óptico cuantificado. Estas propiedades permiten detectar cualquier intercepción o manipulación de la comunicación, de acuerdo con principios fundamentales de la mecánica cuántica, como el teorema de no clonación y el colapso del estado cuántico.

Los equipamientos suministrados tendrán que incluir tanto módulos emisores como receptores, necesarios para establecer conexiones completas entre nodos de la red. Los equipos tienen que estar diseñados para operar en entornos prácticos y reales, y ser compatibles con la infraestructura de red definida en este proyecto.

Además, los equipos tienen que incorporar un módulo de generación de aleatoriedad cuántica (QRNG) como fuente de alta entropía para la generación o inicialización de claves. Este subsistema proporciona números aleatorios genuinos, no predictibles, garantizados por fenómenos cuánticos físicamente verificables, y forma parte integrante del sistema conjunto de QKD y KMS. Su presencia es necesaria para asegurar niveles avanzados de seguridad criptográfica en entornos integrados.

3.1.1. Compatibilidad e integración

Tecnología de modulación:

El sistema tendrá que basarse en CV-QKD con esquema Prepare-and-Measure, e implementar protocolos de modulación gausiana de estados coherentes (GMCS).

Los equipos QKD tienen que cumplir con los requisitos siguientes para garantizar su integración en entornos reales y heterogéneos:

- Compatibilidad óptica:
    - Los equipos tendrán que garantizar también la coexistencia del canal cuántico con datos en banda C estándar (1530–1565 nm), asegurando la interoperabilidad y la calidad del servicio en escenarios mixtos.
    - Soporte para transmisión conjunta de canales cuántico y clásico sobre una única fibra óptica, con el uso de técnicas de multiplexación WDM sin degradación significativa de rendimiento.

- Interoperabilidad con infraestructuras de red:
    - Compatibilidad con sistemas DWDM y CWDM, especificando las longitudes de onda exactas compatibles.
    - Capacidad para personalizar la longitud de onda del canal cuántico.
    - Los equipos tendrán que permitir la co-propagación con al menos 4 canales DWDM de servicio de cliente, sin degradación significativa del rendimiento del sistema QKD.

- Cumplimiento de los estándares ETSI GS QKD 004 y 014, así como ITU-T Y.3800.
- Soporte para interfaces de gestión estándar, como SNMP y HTTP.
- Capacidad de operación en escenarios punto-a-multipunto (P2MP).

- Flexibilidad y mantenimiento:
  - Posibilidad de sustituir independientemente cualquiera de los dispositivos (emisor o receptor) sin requerir la sustitución de toda la pareja.
  - No se aceptarán sistemas vinculados por parejas fijas de fábrica que obliguen a la renovación completa del sistema en caso de fallo parcial.

- Integración con sistemas de gestión de claves (KMS):
  - Conexión directa o indirecta con el KMS mediante APIs compatibles (RISTRE, JSON-RPC, KMIP).
  - Soporte para protocolos de entrega de claves compatibles con ETSI GS QKD 004 y 014.

- Seguridad y coherencia tecnológica:
  - Garantía de compatibilidad criptográfica y de seguridad entre dispositivos de una misma serie, modelo o familia tecnológica del fabricante.

3.1.2. Rendimiento y funcionalidad

Los sistemas tendrán que cumplir los siguientes requisitos mínimos con respecto al rendimiento, fiabilidad y capacidad operativa:

- Rendimiento criptográfico y de transmisión
  - Pérdida óptica máxima tolerada: mínimo 10 dB.
  - Presupuesto en potencia: máximo de -10 dBm (10mW).
  - Tasa mínima de generación neta de claves simétricas:
    - ≥ 1 kbps por pareja emisor/receptor en condiciones de enlace estándar (10 dB).
    - ≥ 25 bps por servicio con solicitud del KMS cada 10 s.
    - ≥ 500 bps en escenarios multiusuario y condiciones de red máximas previstas (16 dB).

    Nota: la tasa de generación de claves se tendrá que expresar también en términos de claves AES generadas por hora por pareja de nodos, indicando explícitamente el presupuesto en potencia correspondiente. El sistema tendrá que alcanzar, como mínimo, 7.000 claves AES/hora @ 10 dB, y hasta 10.000 claves AES/hora @ 16 dB en condiciones óptimas.

- Fiabilidad, autonomía y seguridad operativa
    - El sistema ha de:
        - Funcionar de manera autónoma y continua, sin dependencias externas críticas.
        - Permitir configuración como fuente primaria o secundaria (redundante) de entropía.
        - Disponer de mecanismos de contingencia en caso de fallo de la fuente cuántica (bloqueo de flujo, alertas, etc.); queda prohibido generar datos sintéticos de forma automática.

- Operatividad y gestión
    - Soporte para:
        - Regeneración automática de claves y recuperación automática ante errores o interrupciones.
        - Actualización remota y segura del firmware.
    - Se tiene que entregar documentación técnica completa y manuales operativos en catalán.

- Escalabilidad futura
    - Capacidad para evolucionar hacia entornos con:
        - Integración de tecnologías post-cuánticas híbridas.
        - Soporte a arquitecturas SDN/NFV y escenarios de carga elevada.

3.1.3. Formato físico e instalación

El equipo deberá tener un formato integrable en racks de 19”, con una profundidad máxima de 600 mm y una altura máxima de 2U por unidad principal. Se podrá admitir 1U adicional para equipo auxiliar justificado (p.ej. alimentación, supervisión, etc.).

Deberá ser compatible con la instalación en armarios estándar de telecomunicaciones.

3.1.4. Comunicación y canales

Los equipos QKD tienen que cumplir los requisitos siguientes con respecto a la comunicación y transmisión de señales:

- Canal clásico de comunicación
    - Utilizar conectividad TCP/IP estándar sobre interfaces RJ45 o SFP/SFP+ compatibles.
    - Compatibilidad con la transmisión conjunta de datos convencionales (canales mixtos), sin interferencias.

- Canal de sincronización
    - La sincronización se tiene que integrar en el canal de datos, sin requerir canales físicos independientes.

- Tolerancia y robustez de transmisión
    - El sistema tiene que soportar enlaces con un presupuesto total de pérdidas ópticas ≥ 18 dB, asegurando operatividad en escenarios con infraestructura variable o ampliable.
    - Deberá tolerar potencias inyectadas > 5 dBm procedentes de canales clásicos adyacentes, sin degradación de la funcionalidad cuántica.

3.1.5. Gestión, control y monitorización

Los equipos tienen que disponer de funcionalidades avanzadas de supervisión y gestión operativa, incluyendo:

- Control remoto y gestión segura a través de protocolos e interfaces estándar como:
    - SSH, SNMPv3, REST API, o Netconf/YANG.

- Monitorización en tiempo real de parámetros críticos como:
    - Pérdidas ópticas, ruido, potencia de señal recibida, entre otros.
    - Valores específicos de distribución de claves cuánticas, incluyendo la Secure Key Rate (SKR), y el Excess Noise, de acuerdo con los protocolos CV-QKD implementados.

- Registro completo de actividad (logs) con capacidad de exportación de auditorías para seguimiento y trazabilidad de los eventos del sistema.
    - Los dispositivos y componentes tendrán que exportar sus registros de forma continua hacia las plataformas de recolección del CTTI y de la Agencia de Ciberseguridad para su análisis y correlación.

- El sistema tendrá que incluir también un sistema de alertas específico sobre el rendimiento y el estado del hardware, incorporando como mínimo el consumo de CPU, la latencia en la distribución de claves y las condiciones ambientales de temperatura y humedad.

- La solución se tendrá que integrar con las herramientas de monitorización y observabilidad del CTTI.

- Los equipos tendrán que incluir como mínimo las siguientes interfaces físicas:
    - 1 puerto cuántico dedicado a la transmisión del canal cuántico.
    - 1 puerto Ethernet por conexión de gestión y transmisión clásica.
    - 1 puerto de consola por configuración directa local (ex.: RS232, USB o similar).

3.1.6. Seguridad

Los equipos deberán incorporar medidas avanzadas para garantizar la integridad, confidencialidad y robustez del sistema:

- Protección contra ataques de canal lateral conocidos, incluyendo manipulaciones del 'local oscillator' y ataques basados en medidas.
- Las claves generadas deberán ser aleatorias e incondicionalmente seguras, conforme a los modelos de seguridad reconocidos por organismos internacionales.
- Requisitos específicos de protección física y supervisión:
    - Mecanismos de detección automática de fallos o manipulaciones (self-check, watchdogs, etc.).
    - Registro de fallos con notificaciones inmediatas por SNMP, API o consola local.
- El sistema QKD tendrá que garantizar que el valor del parámetro de seguridad ε sea menor o igual a 10^{-9}, de acuerdo con las prácticas habituales y los estándares internacionales en QKD.

3.1.7. Certificación y normativas

Los equipos tienen que cumplir con los requisitos siguientes para garantizar la calidad y la seguridad de la fuente de entropía:

- Disponer de certificación o validación por terceros independientes, basada en:
    - Tests estadísticos estandarizados reconocidos, como NIST SP 800-90B, DieHarder, TestU01 o equivalentes.
    - Preferentemente, certificación Common Criteria o acreditación por agencias oficiales como ANSSI, NIST, CCN o similares.

3.2. Equipamientos KMS

Subsistema encargado de la generación, distribución, almacenaje, rotación, recuperación y revocación de claves criptográficas en un entorno seguro. Actúa como componente central de la infraestructura de gestión de claves, facilitando la integración de servicios de cifrado y firma digital, tanto en entornos clásicos como en sistemas con soporte para tecnologías de distribución de claves cuánticas (QKD).

3.2.1. Compatibilidad y protocolos

- El KMS tendrá que ser plenamente compatible con sistemas QKD basados en protocolos de distribución cuántica, incluyendo:
    - CV-QKD (Continuous Variable)
    - DV-QKD de variable discreta (compatibilidad híbrida futura)

- Tendrá que incorporar funcionalidades operativas específicas, como:
    - Quantum-safe Key Relay entre nodos, con implementación de los estándares ETSI GS QKD 015, que garantice la distribución y retransmisión segura de claves en entornos híbridos clásicos y cuánticos, y que incorpore un mecanismo explícito de gestión y ejecución del relay (por ejemplo, establecimiento de canales seguros autenticados y protocolos de retransmisión verificables).
    - Fuente de entropía interna basada en QRNG, con disponibilidad de mecanismos de generación alternativos (fallback) que aseguren la continuidad del servicio en caso de fallo de la fuente principal.
    - Cumplimiento de los estándares de seguridad FIPS 140-2 o FIPS 140-3, o bien certificación Common Criteria EAL2+ para los módulos criptográficos internos (HSM).
    - Enrutamiento redundante de claves y almacenaje seguro.
    - Alta disponibilidad (HA) a nivel de nodo QKD.

- Integración con el plano de control de QKD por vía de interfaces estándar:
    - ETSI GS QKD 014 (todos los métodos), incluyendo SKIP, por interfaces API/KMI.
    - Otros estándares como ETSI GS QKD 004.
    - Soporte para QKD Network Layer (QNL) por topología multipunto.

- Cumplimiento de los protocolos de gestión de claves más habituales:
    - PKCS#11, y compatibilidad con arquitecturas HSM.
    - El KMS tendrá que estar basado en un sistema operativo Unix o similar, que garantice estabilidad, seguridad y compatibilidad con entornos de red y gestión de claves.

- El KMS tendrá que ser interoperable con:
    - Equipos QKD de múltiples fabricantes (estándares ETSI/ITU).
    - Sistemas criptográficos clásicos (TLS/IPsec), y soluciones híbridas post-cuánticas.

- El sistema tendrá que permitir también:
    - Soporte de múltiples módulos QKD en un mismo nodo, con capacidad para gestionar en concurrencia un mínimo de 5 módulos QKD y 5 instancias de KMS de manera simultánea.
    - Hibridación de claves PQC/QKD.

- El KMS tendrá que soportar mecanismos de establecimiento de claves simétricas (SKE) y permitir la combinación criptográfica de claves obtenidas mediante SKE, protocolos QKD y unos o más algoritmos de Criptografía Post-Cuántica (PQC), facilitando la implementación de agilidad criptográfica y estrategias de defensa en profundidad ante amenazas presentes y futuras.

3.2.2. Capacidades y gestión de claves

- Capacidad para distribuir claves generadas a través de QKD hacia múltiples destinatarios de manera segura, escalable y trazable.
- Capacidad para distribuir, gestionar y entregar claves simétricas de diferente naturaleza criptográfica (clásica, PQC y QKD), de acuerdo con las políticas definidas e independientemente del mecanismo de generación o establecimiento.
- Soporte para:
    - Clave unicast, multicast y broadcast.
    - Clave por servicio, por sesión y por dispositivo.

- Capacitado para operar tanto en modo P2P como en topología en estrella, hub&spoke o malla.
- Integración con sistemas de identidad y control de acceso:
    - LDAP, RADIUS, SAML o protocolos OAuth2/OpenID Connect.

- Posibilidad de definir políticas de control de acceso basadas en roles (RBAC).
- Soporte paraautenticación mutua entre entidades (MFA, certificados digitales, etc.).
- Las interfaces del KMS tendrán que protegerse mediante HTTPS sobre TLS 1.3 (RFC 8446), con autenticación mutua basada en certificados X.509, de acuerdo con los requisitos del estándar ETSI GS QKD 014.
- Sistema de copia de seguridad automática y restauración segura, con cifrado de las claves en reposo y en tránsito.
- Las copias se tienen que poder realizar:
    - Localmente, en dispositivo físico (ex. HSM secundario).
    - Remotamente, con canales seguros (VPN, TLS 1.3).

- Las claves en backup tienen que disponer de protección por hardware (HSM y módulos TPM) o bien de un sistema equivalente de protección criptográfica.
- El sistema tendrá que garantizar un ciclo de vida completo de las claves (generación, distribución, uso, rotación, revocación y destrucción), que sea seguro y configurable según las políticas del CTTI y los estándares internacionales.

3.2.3. Seguridad y supervisión

- Los sistemas KMS tienen que estar protegidos contra:
  - Acceso físico no autorizado (anti-tampering, carcasa blindada si es HW).
  - Ataques lógicos (DoS, side-channel, ataque por inyección de comandos).

- Tienen que incluir:
  - Monitorización de integridad y mecanismos de verificación (ex. checksums, firmware firmas).
  - Soporte para logging criptográficamente firmado.

- Registro completo de actividades y accesos con:
  - Logs detallados de operaciones de generación, distribución y uso de claves.
  - Posibilidad de integración con sistemas SIEM (Security Information and Event Management).

- Interfaz de gestión con monitorización en tiempo real de los siguientes parámetros:
  - Estado de nodos, transacciones de clave, errores y acontecimientos de seguridad.
  - Parámetros específicos de claves: Secure Key Rate (SKR), Effective Secure Key Rate (ESKR), número de claves almacenadas y número de claves consumidas.
  - Soporte para monitorización mediante SNMP (Simple Network Management Protocolo), por integración con sistemas de supervisión de red.
  - El sistema tendrá que disponer también de una interfaz gráfica de administración basada en WebUI, accesible de manera segura mediante navegador, que permita la gestión y monitorización de todas las funcionalidades del KMS.

- Requerimientos mínimos de conectividad física:
  - 3 puertos Ethernet para conexiones de red y un puerto de consola por gestión directa.

- El KMS tendrá que permitir la segmentación lógica o física del tráfico entre los canales de gestión, entrega de claves, recogida de claves y comunicación con otros KMS, para garantizar el aislamiento y la seguridad de cada flujo.

3.3. Garantías extendidas y servicio de mantenimiento

Los equipamientos suministrados tendrán que cumplir los requisitos con relación a sus garantías extendidas, así como su servicio de mantenimiento:

Garantías extendidas

- Los equipos (hardware, software y licenciamiento) tendrán que disponer de garantía extendida del fabricante durante un mínimo de cinco (5) años a partir de la fecha de aceptación definitiva del suministro.
- El adjudicatario tendrá que activar las garantías extendidas de los fabricantes, a nombre del CTTI, en el momento en que los equipos se pongan en producción.
- Las garantías extendidas tendrán que cubrir todo el soporte técnico necesario para el correcto funcionamiento de la solución y la incorporación de nuevas funcionalidades, así como la sustitución de equipamientos defectuosos in situ sin ningún coste adicional para el CTTI.
- El adjudicatario será responsable de la gestión integral de las garantías extendidas con los fabricantes y de la interlocución con el CTTI y/o con los proveedores que éste designe.
- El CTTI podrá autorizar a otros gestores para que, durante la vigencia del contrato o posteriormente, puedan gestionar directamente con los fabricantes las garantías extendidas (recambios, soporte, etc.).

Servicio de mantenimiento

- El adjudicatario tendrá que prestar servicio de mantenimiento integral de todo el hardware, software y licenciamiento suministrado, desde la aceptación definitiva hasta la finalización del contrato.
- El servicio incluirá intervenciones remotas e in situ, según sea necesario.
- Las actividades mínimas incluidas serán:
    - Soporte técnico (correo electrónico, teléfono, reuniones telemáticas o presenciales, herramientas internas CTTI).
    - Interlocución con los fabricantes y gestión de garantías extendidas.
    - Análisis e implementación de nuevas funcionalidades.
    - Actualizaciones de firmware y software (plan de versiones).

  - Revisiones y actuaciones preventivas (plan de mantenimiento preventivo).
  - Actuaciones correctivas: reparación o sustitución de cualquier elemento defectuoso.
  - Intervenciones programadas y de urgencia, de acuerdo con el procedimiento de gestión de cambios del CTTI.
  - Generación de informes periódicos del servicio de mantenimiento.

- Tiempo de respuesta y resolución:
  - Las actuaciones correctivas de urgencia tendrán que ejecutarse y resolver la incidencia o problema en un plazo máximo de 24 horas laborables desde la notificación.
  - En caso de fallo grave o irreparable, habrá que proporcionar un equipo de sustitución equivalente o superior en un plazo máximo de 7 días naturales.

- Niveles soporte:
  - Nivel 1 (L1): Atención inicial y resolución de incidencias en primera instancia. Atención y resolución de incidencias, peticiones y gestión proactiva de alertas del sistema de monitorización.
  - Nivel 2 (L2): Soporte técnico avanzado. Intervenciones in situ y sustitución de hardware. Escalado al nivel 3 cuando sea necesario.
  - Nivel 3 (L3): Soporte técnico del fabricante para incidencias críticas o de máxima complejidad, así como nuevas evoluciones.

- El adjudicatario tendrá que facilitar las hojas de ruta de los fabricantes con relación a actualizaciones tecnológicas y soporteevolutivo de hardware, software y licenciamiento, como mínimo, semestralmente o bien en el momento en que haya algún cambio relevante.

4. CONDICIONES DE EJECUCIÓN DEL SERVICIO

4.1. Estructura organizativa

Dentro de este capítulo se definen los perfiles que tienen que formar la estructura organizativa que proponga el licitador, así como de forma ilustrativa las principales funciones, entre otras, que deberán desarrollar.

Los recursos humanos asignados por el adjudicatario deberán poseer la calificación necesaria para poder garantizar con éxito la implantación del proyecto 'Encriptación Cuántica Generalitat de Catalunya'.

El CTTI se reserva el derecho de pedir el cambio de algún recurso si detecta que no es capaz de cumplir con las mínimas exigencias que son necesarias. En este caso, el adjudicatario tendrá que presentar un plan de cambio del recurso o recursos, que tendrá que ser aprobado por el CTTI.

Composición de los puntos para facilitar la comprensión de las necesidades demandas:

- Funciones de los perfiles: Incluye el detalle de las responsabilidades que tendrán que asumir los perfiles según las funciones asignadas.
- Idoneidad de los perfiles: Incluye las características académicas y experiencia profesional que tendrá que cumplir cada perfil.
- Propuesta técnica y organizativa: Incluye el detalle de los perfiles del equipo técnico que el licitador considere más adecuado para la implantación del proyecto 'Encriptación Cuántica Generalitat de Catalunya'.

4.1.1. Funciones de los perfiles

Las funciones mínimas que tendrán que asumir estos perfiles para la correcta implantación de la solución son las siguientes:

- **Responsable de cuenta:** Este perfil corresponderá al responsable máximo (del contrato) del adjudicatario enfrente del CTTI, velando por que éste se cumpla.

  Principalmente es el responsable máximo de los ámbitos económico, contractuales, organización y estrategia de prestación del servicio.

- **Jefe de proyecto**: Será la persona encargada de planificar, dirigir, supervisar y coordinar todas las actividades relacionadas con los proyectos, servicios y suministros asociados, incluyendo el análisis y gestión de desviaciones de alcance, costes y plazos. Gestionará los recursos asignados, el seguimiento de riesgos y cambios, y la coordinación con otros proveedores o terceros involucrados.

  Realizará funciones de dirección, planificación estratégica, control y supervisión tanto de la ejecución técnica como del equipo humano implicado en la implementación y operación de los sistemas de comunicación cuántica, garantizando el cumplimiento de los requisitos funcionales, de calidad y de seguridad establecidos.

Será la persona que tendrá que asegurar el éxito del servicio y los proyectos de los que será responsable, certificando su correcta ejecución, así como el cumplimiento de los requerimientos y objetivos marcados por el cliente y que tendrán que cubrir toda una serie de necesidades.

- **Arquitecto**: Perfil responsable del diseño de la arquitectura global de la red, integrando tanto los elementos clásicos de comunicación como los dispositivos y protocolos de comunicación cuántica. Su función será asegurar la coherencia técnica, la compatibilidad entre sistemas y la seguridad en todo el diseño, teniendo en cuenta los requisitos específicos de la tecnología QKD, (Continuous Variables – CV-QKD) y sistemas de gestión de claves (KMS). Referente tecnológico de las actividades de arquitectura y soluciones tecnológicas en el ámbito de los servicios objeto de esta licitación.

  El personal con las funciones de arquitecto tendrá como principales tareas / responsabilidades:

  - Validar el diseño (a nivel tecnológico) que permita llenar a todas y cada una de las necesidades que vayan apareciendo.
  - Aportar, proponer y desarrollar las mejoras a nivel de arquitectura.
  - Junto con el responsable técnico, será el encargado de dar cobertura a la necesidad de funciones avanzadas, como Servicios profesionales de tercer nivel en el Soporteal diseño de soluciones tecnológicas y otros que considere el CTTI.

- **Administradores de redes y comunicación cuántica**: Responsables de todas las tareas de administración, procedimientos y revisión (optimización) de la red (equipamiento físico, virtual o en el cloud), incluyendo todas las tareas necesarias para la ejecución de los servicios definidos para un administrador de red y seguridad.
- **Operadores de red y seguridad:** Este perfil corresponde a técnicos responsables de tareas de administración básica, operación y monitorización en tiempo real de la infraestructura de redes de comunicaciones y servicios de seguridad asociados. Serán responsables de la supervisión de elementos de red y de comunicación cuántica, la gestión de incidencias de primer nivel, alarmas y notificaciones de errores, el escalado y la actualización del estado de los servicios y sistemas, así como el registro y documentación de operaciones y eventos.
- **Ingeniero/a de seguridad y criptografía:** Perfil encargado de garantizar que la infraestructura desplegada cumple los requerimientos de seguridad en todo el ciclo de vida del sistema, especialmente con respecto a la protección de la información, la integración del sistema de distribución de claves cuánticas (QKD) con el sistema de gestión de claves (KMS), y la interoperabilidad con sistemas clásicos de cifrado.

- **Coordinador/a de integración y pruebas:** Perfil responsable de diseñar, planificar y supervisar la realización de pruebas de sistema, incluyendo pruebas de rendimiento, interoperabilidad, estabilidad y seguridad en las fases de despliegue y validación de la nueva infraestructura. Coordinará a los diferentes actores técnicos implicados y será responsable de validar la correcta integración de los sistemas de comunicación cuántica con el resto de la red.

- **Servicios profesionales de tercer nivel:** Este perfil actuará en colaboración con el equipo técnico del cliente y será el enlace con el soporte de nivel máximo del fabricante. Su participación será crítica en fases de puesta en producción, resolución de incidencias de máxima complejidad y mantenimiento evolutivo.

  Encargado de dar cobertura a todas las fases para la implantación de la solución. Estos recursos estarán a disposición del CTTI para poder ser utilizados principalmente en las siguientes casuísticas:

  - Soporteal diseño de soluciones tecnológicas.
  - Certificación del diseño propuesto.
  - Auditoría del despliegue de la solución.
  - Agilizar la interlocución interna del fabricante.
  - Participación en el proceso de preparación y migración de los datos en la nueva solución.
  - Soportea los cambios que considere el CTTI.
  - Resolución de las incidencias.

Estos perfiles descritos equivalen a los siguientes del informe justificativo:

Perfil	Perfil equivalente
Responsable de cuenta	Arquitecto
Jefe de proyecto	Jefe de proyecto
Arquitecto	Arquitecto
Administradores de redes y comunicación cuántica	Administrador
Operadores de red y seguridad	Operador
Ingeniero de seguridad y criptografía	Administrador
Coordinador de integración y pruebas	Administrador

4.1.2. Idoneidad de los perfiles

A continuación, se detallan los perfiles principales con las características mínimas que tendrán, aunque también tendrá que incluir las funciones descritas en el apartado 4.1.1

Funciones de los perfiles según corresponda tal como está detallado en 4.1 Estructura Organizativa:

- **Responsable de cuenta**:

  La persona asignada tendrá que disponer, como mínimo, de una titulación universitaria superior (preferentemente en Ingeniería, Ciencias o Tecnologías de la Información) o, alternativamente, acreditar una experiencia mínima de 5 años en la gestión y coordinación de servicios o proyectos TIC de elevada complejidad, preferentemente en entornos del sector público.

  Deberá acreditar experiencia específica en la relación con clientes institucionales y en la coordinación transversal con equipos técnicos, así como en la gestión de incidencias, riesgos y comunicación con múltiples actores.

  La comunicación fluida, la proactividad, la capacidad de negociación, la flexibilidad y la adaptabilidad son competencias fundamentales de este perfil.

- **de proyecto**:

  - Titulación mínima: Grado o licenciatura de ámbito tecnológico, preferentemente en Ingeniería de Telecomunicaciones, Ingeniería Informática o titulaciones afines.
  - Experiencia mínima: Al menos 5 años de experiencia acreditada en la dirección de proyectos complejos en el ámbito de las redes de telecomunicaciones, especialmente en entornos con tecnologías ópticas, requisitos de seguridad elevada, o sistemas de alto rendimiento y disponibilidad.

- **Arquitecto**:

  - Experiencia mínima: 5 años en el diseño de arquitecturas de redes complejas, preferentemente en entornos críticos o de seguridad elevada, con al menos 2 años en la integración de soluciones de comunicación cuántica o participación directa en pilotos o proyectos con esta tecnología.
  - Conocimientos específicos requeridos:
    - Diseño de arquitecturas de red para soluciones híbridas clásicas/cuánticas.
    - Conocimiento de fabricantes y soluciones de comunicación cuántica.

- Conocimiento de protocolos de distribución de claves cuánticas (QKD), CV-QKD, y gestión criptográfica asociada (KMS).

- Certificaciones mínimas o equivalentes:
  - Cisco Certified Design Profesional (CCDP) o NSE 7 de Fortinet, como demostración de habilidades en diseño y seguridad de red.

- **Administradores de redes y comunicación cuántica**:
  - Experiencia mínima: 3 años en administración de redes de comunicaciones de alta disponibilidad y rendimiento, preferentemente en entornos públicos o críticos, y participación (aunque sea parcial) en proyectos relacionados con la comunicación cuántica.
  - Conocimientos requeridos:
    - Protocolos de routing: IS-IS, OSPF, RIP, EIGRP, BGP por IPv4 y IPv6.
    - Servicios de nivel 2: Ethernet Virtual Circuitos (EVC, QinQ, 802.1ad, EFP), clasificación de VLAN, IEEE Bridging, 802.1s MST, 802.1w RSTP, MST Access Gateway.
    - Configuración, diagnóstico y despliegue básico de sistemas de comunicación cuántica.
    - Conocimiento de los requisitos de interoperabilidad con dispositivos QKD y compatibilidad con KMS.
  - Certificaciones mínimas:
    - Cisco Certified Network Profesional (CCNP Routing & Switching), o equivalente como NSE 3 de Fortinet.

- **Operadores de red y seguridad:**
  - Titulación mínima: Formación profesional de grado medio o superior en informática, telecomunicaciones o equivalente.
  - Experiencia mínima: 2 años en tareas de operación y monitorización de redes de comunicaciones y sistemas de seguridad en entornos operativos reales.

- **Ingeniero/a de seguridad y criptografía:**
    - Titulación mínima: Grado o licenciatura en Ingeniería Informática, de Telecomunicaciones, Matemáticas o similar.
    - Experiencia mínima: 3 años proyectas seguridad de red y criptografía.
    - Conocimientos requeridos:
        - Protocolos criptográficos (TLS, IPSec, VPNs, etc.).
        - Sistemas de gestión de claves (KMS, HSM).
        - Conocimiento de criptografía post-cuántica y de protocolos de distribución de claves cuánticas (QKD).
        - Normativas y buenas prácticas (ISO/IEC 27001, CCN-STIC, etc.).

- **Coordinador/a de integración y pruebas:**
    - Titulación mínima: Grado en Ingeniería o equivalente.
    - Experiencia mínima: 4 años en proyectos TIC complejos con pruebas de integración de sistemas.
    - Conocimientos requeridos:
        - Metodologías de test (Test Plans, Use Cases, Acceptance Criteria...).
        - Conocimiento de herramientas de monitorización y simulación de red.
        - Conocimiento de protocolos de red y, preferentemente, de sistemas QKD/KMS.

- **Servicios profesionales de tercer nivel:**

  Este perfil corresponde al de un técnico o ingeniero de alto nivel, especializado en los sistemas y equipos suministrados, con capacidad para intervenir en tareas de diagnóstico, resolución de incidencias graves, optimización e integración personalizada de soluciones, tanto en el ámbito de la red como de la comunicación cuántica.
    - Requisitos:
        - Certificación de nivel máximo disponible por parte de los fabricantes de los sistemas que se ofrecen (ex: Cisco CCIE, Fortinet NSE 8, etc.) o, en el caso de soluciones de comunicación

cuántica, acreditación directa y formal de formación, capacitación o colaboración oficial con el fabricante de la tecnología QKD o KMS propuesta.

- Experiencia demostrada en el despliegue o soporte experto de soluciones equivalentes en entornos operativos.

- Obligaciones del licitador:
  - Indicar claramente en la propuesta los recursos que se asignarán a este servicio.
  - Aportar CV, certificaciones y referencias de proyectos previos similares con soluciones de comunicación cuántica o redes de alta seguridad.
  - Garantizar disponibilidad en casos de soportecrítico y compatibilidad idiomática con el equipo del cliente.

4.1.3. Dimensionado organizativo

A título orientativo, se presenta a continuación la composición mínima del equipo, que podrá participar en todas las fases o solo en alguna de ellas:

Clasificación perfiles	Funciones Perfil	Recurrente
Responsable de Cuenta	Responsable de Cuenta	1
de proyecto	de proyecto	1
Arquitecto de red y comunicación cuántica	Arquitecto	1
Administrador de redes y comunicación cuántica	Administrador	2
Operador de red y seguridad	Operador	2
Ingeniero/a de seguridad y criptografía	Experto en criptografía, KMS y protocolos	1
Coordinador/a de integración y pruebas	Coordinador de test y validación funcional	1
Servicios profesionales de tercer nivel	Técnicos con máxima certificación / experto	1

El adjudicatario tendrá que proporcionar servicios profesionales de terceros con un mínimo de 100 horas durante el contrato.

Dada la rápida evolución de la tecnología, estos perfiles se pueden cambiar por perfiles equivalentes necesarios, siempre previa validación del CTTI.

Cualquier cambio en estos recursos asignados al servicio tendrá que ser comunicado previamente al CTTI, que tendrá que dar su visto bueno, sin el cual no se podrá llevar a cabo el cambio y por lo tanto el adjudicatario tendrá que buscar una alternativa.

En caso de sustitución de algún otro componente del equipo presentado, el sustituto tendrá una idoneidad equivalente o superior a la presentada en la oferta.

4.1.4. Cláusula de seguridad

Confidencialidad

Todo el personal de la empresa adjudicataria, así como los posibles subcontratistas tienen el deber de mantener absoluta confidencialidad y estricto secreto sobre la información conocida a raíz de la ejecución de los servicios contratados. Esta obligación de confidencialidad se tendrá que mantener durante 5 años, o lo que se especifique en el contrato, desde que se tuvo conocimiento de la información, excepto en relación con los datos personales a las que accedan con respecto a las que habrá que mantener el deber de confidencialidad de manera indefinida, subsistiendo incluso cuando se finalice la relación contractual, según establece la Ley Orgánica 3/2018.

La empresa tiene que comunicar esta obligación de confidencialidad a su personal, ya sea interno como externo, que esté involucrado en la ejecución del contrato y posibles subcontratistas y tiene que controlar su cumplimiento.

La empresa adjudicataria tiene que poner en conocimiento del CTTI, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar a la integridad o la confidencialidad de la información.

Conformidad con el Esquema Nacional de Seguridad

De conformidad con el artículo 2 del Real decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (de ahora en adelante, ENS o RD 311/2022), el adjudicatario tiene que estar en condiciones de poder evidenciar la conformidad con el ENS de los sistemas de información sobre los que se sustenten los servicios objeto del contrato (suministro, puesta en marcha y mantenimiento), requiriéndose que presente el Certificado de Conformidad con el ENS en categoría **MEDIA**, o superior, de los sistemas que intervengan en la prestación de los servicios indicados antes del inicio de la prestación.

El adjudicatario tendrá que mantener la conformidad vigente durante todo el ciclo de vida del contrato. La pérdida o retirada temporal de la conformidad se tendrá que comunicar de manera inmediata y sin dilación indebida en el CTTI, que tendrá que considerar el impacto en el contrato de esta circunstancia.

La renovación de la conformidad durante la vigencia del contrato se notificará inmediatamente, incluyendo el proceso de adaptación del sistema de información al Real decreto 311/2022.

Adicionalmente, el adjudicatario, tendrá que notificar al inicio de la prestación la identidad y datos de contacto de la persona que asumirá la responsabilidad de Punto o Persona de Contacto (POC), según lo que dispone el artículo 13.5 del Real decreto 311/2022, así como la declaración en que conste la aceptación de la designación y de las funciones específicas. Si durante la ejecución del contrato se produce un cambio en la persona de contacto, se tendrá que notificar de manera inmediata al CTTI, antes de

que finalice la responsabilidad asumida, presentando formalmente la declaración y los datos efectivos de la nueva persona de contacto.

En caso de que exista subcontratación, la empresa adjudicataria tiene que extender estas exigencias a la cadena de suministro, garantizando que las empresas subcontratadas cumplan con el ENS en la categoría requerida.

Además del ENS y la normativa y guías técnicas que lo desarrollan, la empresa adjudicataria del contrato tendrá que conocer y cumplir el Marco Normativo de Ciberseguridad de la Generalitat de Catalunya: https://portal.ciberseguretat.cat y seguir las directrices o instrucciones del CTTI y/o de la Agencia de Ciberseguridad de Cataluña.

Formación del personal

La empresa adjudicataria del contrato tiene que garantizar que todo el personal sea concienciado, reciba formación e información sobre sus deberes, obligaciones y responsabilidades en materia de seguridad derivados de la legislación, del marco normativo interno y de los procedimientos y directrices aplicables, recordando las posibles medidas disciplinarias aplicables y su deber de confidencialidad con respecto a la información a la que tenga acceso.

Adquisición de productos de seguridad

Dado que los productos a suministrar formarán parte de la arquitectura de seguridad de los sistemas de comunicaciones de la Generalitat de Catalunya, a los cuales les corresponde la categoría ALTA del ENS, el adjudicatario tiene que cumplir con la medida *op.pl.5 Componentes Certificados* del anexo II del ENS.

De acuerdo con la medida op.pl.5, se utilizará el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC)** del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema. **En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo con aquello descrito al artículo 19 del ENS.**

En caso de que el producto esté certificado, el adjudicatario tendrá que presentar con detalle todas las características de los productos o servicios y la referencia de la familia donde se haya encuadrado, la categoría acreditada, la fecha de inclusión y la fecha de revisión de validez de la acreditación. El medio por el cual se acredite la seguridad del producto se tendrá que mantener en vigor y actualizado durante toda la vigencia de los derechos de uso de los activos al CTTI. Cualquier cambio en la vigencia de la acreditación tendrá que ser comunicado sin demora.

De manera alternativa, y basándose en el principio de proporcionalidad y neutralidad tecnológica, la arquitectura e infraestructura utilizada en el sistema de información afectado, y considerando los riesgos, los proveedores podrán presentar otras certificaciones de seguridad en que se detallen las funciones de seguridad (como por ejemplo, la certificación emitida por el Esquema Europeo de Certificación de Ciberseguridad o cualquier otro que sea aprobado por la Comisión Europea en virtud

del artículo 49 del Reglamento (UE) 2019/881 relativo al ENISA o la certificación de la ciberseguridad de las tecnologías de la información y la comunicación).

En defecto de certificación, el adjudicatario tendrá que acreditar mediante una declaración de aplicabilidad que el producto o servicio dispone de requerimientos de seguridad equivalentes a los exigidos por el CPSTIC en relación a la familia de productos correspondiendo a su producto y que se pueden consultar en la Guía CCN-STIC 140 "Taxonomía de referencia para productos de seguridad TIC".

En un máximo de 6 meses desde el inicio del contrato, el adjudicatario tendrá que incluir su producto en el CPSTIC.

Verificación del cumplimiento

El CTTI y/o la Agencia de Ciberseguridad de Cataluña, con medios propios o de terceros, podrá auditar la correcta ejecución de los servicios objeto del contrato, en el momento y periodicidad que se estime conveniente. Para este hecho, el adjudicatario garantizará el acceso total a los documentos que se soliciten y herramientas relacionadas, prestará asistencia sin coste adicional, y ejecutará el plan de acción acordado en forma y plazo.

Incidentes de seguridad

El POC tendrá que notificar en el CTTI y en el Catalonia-CERT de la Agencia de Ciberseguridad de Cataluña cualquier incidente de seguridad que pueda redundar, directa o indirectamente, en la seguridad, en los plazos y por las vías que determine o los procedimientos establecidos.

La empresa adjudicataria del contrato tendrá que aportar toda la información necesaria para su gestión y notificación a los organismos competentes y al CTTI. En caso de que sea necesario, la empresa adjudicataria tendrá que colaborar con cualquiera de las tareas que sean requeridas por parte del CTTI y/o por la Agencia de Ciberseguridad de Cataluña para la identificación, contención, erradicación, recuperación y recopilación de las evidencias de los incidentes de seguridad.

5. FASES DE LA PRESTACIÓN DEL SERVICIO

5.1. Fase Plan de migración

Esta fase incluye la definición y concreción del plan de despliegue que definirá los pasos a seguir, así como la temporalidad de cada uno de estos. Incluirá los siguientes puntos:

- Definición concreta de los objetivos de la solución.
- Descripción de la topología.
- Requisitos previos.
- Diseño final de la nueva arquitectura.
- Descripción de las dos fases del despliegue.
- Pruebas y validación.
- Evaluación de riesgos y medidas de mitigación.
- Descripción del cronograma y recursos asociados.

La duración de esta fase será de cuatro (4) meses, a contar desde la fecha de inicio de contrato.

5.2. Fase Ejecución crítica

Suministro e instalación de equipamiento en las sedes y segmentos críticos identificados de los doce nodos previstos, así como en torno al laboratorio.

Las actividades mínimas a realizar serán:

- Suministro de los equipos. Suministro de los equipos necesarios los primeros nodos.
- Despliegue inicial de los equipos. Instalación física de los equipos de los dos primeros nodos y configuración básica puesta en marcha.
- Calibración y paso a producción. Ajuste de las configuraciones de los nuevos equipos y de los equipos existentes para garantizar la comunicación entre extremos y la correcta encriptación.
- Escalado al tercer nodo. Despliegue de los equipos del tercer nodo y evaluación del impacto al complicar la arquitectura de dos a tres nodos y puesta en producción.
- Escalado al resto de nodos. Despliegue del resto de nodos hasta completar los cuatro de esta fase. Evaluación de cómo se comporta esta arquitectura más compleja. Puesta en producción.
- Recogida de datos necesarios para analizar a la fase 'observación y análisis de datos'.

La duración de esta fase será de dieciséis (16) meses, a contar desde la fecha de validación del plan de migración por parte del CTTI.

5.3. Fase Despliegue

Despliegue y ampliación del bloque de comunicaciones encriptado cuánticamente a los 8 nodos restantes. Las actividades a realizar, como mínimo, serán:

- Suministro de los equipos. Suministro de los equipos necesarios los nodos de esta actuación.
- Escalado a cuatro nodos más. Despliegue de cuatro nodos adicionales en base a la experiencia de despliegue de los anteriores y evaluación de posibles incrementos temporales. Evaluación del comportamiento de esta nueva arquitectura, la cual cerraría el anillo metropolitano. Puesta en producción.
- Escalado final. Despliegue de los últimos cuatro nodos y sedes. Evaluación del comportamiento de esta nueva arquitectura, con varias sedes desplegadas conectadas a los nodos y en el anillo. Puesta en producción.
- Mantenimiento del entorno de laboratorio operativo y en ejecución.

La duración de esta fase será de trece (13) meses, a contar desde la fecha de certificación de la puesta en marcha de los nodos asignados en a la fase de ejecución crítica, y la validación explícita por parte del CTTI.

5.4. Fase Análisis de los datos

Observación y análisis de los datos en operación real durante un periodo de tiempo que permita extraer conclusiones relacionadas con el producto evolucionado en el mercado.

La duración de esta fase será de veinticuatro (24) meses, a contar desde la fecha de certificación de la puesta en marcha de los primeros nodos QKD y KMS asignados a la fase de ejecución crítica, y la validación explícita por parte del CTTI.

5.5. Plan de devolución del servicio

El licitador incluirá un Plan de devolución del servicio detallado que describa las obligaciones y tareas que tendrán que ser desarrolladas por cada una de las partes en relación con la devolución, y que incluya los términos y condiciones en que se realizará.

En caso de cese o finalización del contrato, el proveedor estará obligado a devolver el control de los servicios objeto del contrato, teniendo que realizar en paralelo los trabajos de devolución con los de prestación del servicio, sin coste adicional para el CTTI.

Asimismo, se dejará constancia expresa que la adjudicación de este contrato no confiere ningún derecho de propiedad intelectual o industrial a favor de la empresa adjudicataria sobre ninguno de los elementos mencionados, ni sobre los resultados, configuraciones, diseños, desarrollos o conocimiento generado.

Todos los derechos pertenecen exclusivamente al CTTI, y el uso de estos materiales por parte de la empresa adjudicataria quedará limitado estrictamente en el ámbito de ejecución del contrato. Una vez finalizada la relación contractual, la empresa no podrá hacer ningún uso posterior sin autorización expresa y por escrito.

El Plan de devolución tendrá que cumplir, como mínimo, los siguientes principios y contenidos:

- El plazo de ejecución será de entre 2 y 4 meses antes de la finalización del contrato ya sea por haber agotado el plazo o por cancelación anticipada. El CTTI se reserva el derecho de poder reducir el plazo de ejecución según considere necesario.
- Incluirá la metodología de transferencia de conocimiento de los aspectos fundamentales de operación y, como mínimo:

  - Proporcionar, a quien determine el CTTI, de los medios necesarios para la formación de los profesionales del ámbito relacionado con el objeto contractual.
    Esta formación constará de un mínimo de 2 sesiones de 8 horas cada una o equivalente, y cubrirá los siguientes elementos:

    - Formación en los equipos, servicios, funcionalidades, operación y herramientas implantadas, aplicables al diseño escogido. Otras funcionalidades de los equipos y servicios.
    - Aspectos relevantes de los procedimientos del fabricante: roadmap, consultas técnicas, ciclo de vida de los productos, contratos de mantenimientos, etc.
    - Manuales de usuario del servicio con información detallada de las prestaciones y funcionalidades.
    - Documentación de procesos, base de datos de conocimiento, etc.
    - Disponibilidad continua vía web.

    Toda la formación y documentación necesaria será proporcionada, al menos, en idioma catalán.

  - El acceso al hardware, el software, la información, la documentación y otro material utilizado por el adjudicatario o la Generalitat de Catalunya en la provisión del servicio.
  - La formación práctica tutelada, en la cual el personal designado por el CTTI realice los trabajos propios de cada proceso o funcionalidad tutelados por el personal del adjudicatario.

- El adjudicatario tendrá que ofrecer el hardware y los equipos informáticos, adscritos de forma exclusiva a los servicios objeto del contrato, al CTTI o a terceras partes por éste. La valoración de los equipos se realizará por uno

tercero utilizando el criterio de “precio de mercado” o, si no es posible, sustrayendo a su precio de compra el coste de la amortización sin valor residual. El CTTI, o terceras partes por éste, podrá realizar la compra de todos o parte de los equipos.

- El CTTI podrá suscribir un contrato de licencia de uso sobre los sistemas del adjudicatario que fueran necesarios para asegurar la continuidad del servicio.
- El adjudicatario tendrá que ofrecer toda la ayuda en la transferencia al CTTI, o a terceras partes designadas por éste, de servicios subcontratados, garantías o contratos de mantenimiento existentes hasta el momento de la terminación en los mismos términos pactados con los adjudicatarios de estos.
- El adjudicatario tendrá que ofrecer un Plan para definir las responsabilidades y gestionar la resolución de problemas entre el nuevo adjudicatario, el CTTI y/o otros adjudicatarios.
- Durante el periodo de devolución del servicio, el adjudicatario tiene que cumplir los Acuerdos de Nivel de Servicio. El Plan de devolución no tiene que causar ninguna discontinuidad en el servicio.
- El CTTI no asumirá una dedicación significativa de recursos propios o de la Generalitat de Catalunya en las actividades de devolución.
- El adjudicatario tendrá que garantizar que se dispone de la documentación actualizada de la gestión del servicio (base de datos de conocimiento) a transferir.
- Antes del inicio de la fase de devolución, el adjudicatario tiene que garantizar, para los sistemas de información de importancia Alta, que la documentación base se encuentra actualizada. Se considera documentación base la que se encuentra indicada como grado de necesidad imprescindible a: *https://qualitat.solucions.gencat.cat/guies/transicio/lliurables_transicio_devolucio/)*

Le corresponde al adjudicatario del contrato liderar y asegurar la calidad y transparencia del proceso de devolución del servicio.

La devolución del servicio por parte del adjudicatario saliente incluye dos fases:

- **Prestación en devolución:** durante la ejecución del Plan de devolución el adjudicatario saliente tiene que asegurar la continuidad del servicio con el cumplimiento de los ANS establecidos para cada uno de los servicios y todas las responsabilidades para su correcta ejecución, tal como se especifica en este . El adjudicatario saliente es plenamente responsable del servicio.
- **Devolución del servicio**: a la vez que el adjudicatario saliente sigue prestando el servicio bajo las condiciones expresadas en el presente , tendrá que asegurar un correcto traspaso de la información y de los servicios a quien determine el CTTI.

6. ACUERDOS DE NIVEL DE SERVICIO (ANS)

6.1. Objetivo

Se describe el modelo de Acuerdo de Nivel de Servicio (en adelante ANS), que define los indicadores y los niveles de servicio exigidos, y establece una base objetiva y medible que refleje el compromiso entre el adjudicatario y el CTTI para prestar los servicios requeridos de forma satisfactoria a la Generalitat de Catalunya. El CTTI hará el seguimiento de la calidad del servicio y evaluará periódicamente el servicio prestado por el adjudicatario.

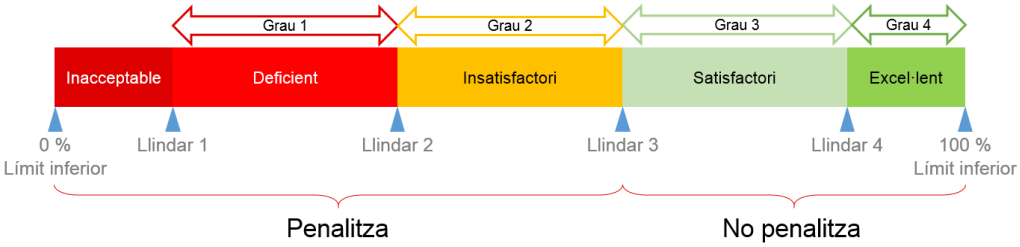
El CTTI pretende obtener un nivel de servicio de alta calidad, así como un grado de satisfacción elevado por parte de los usuarios, basado en:

- El establecimiento de indicadores de servicio, de manera que el CTTI pueda realizar una evaluación objetiva del servicio y sus entregables, y que el adjudicatario tenga una base para la corrección de las eventuales deficiencias en la prestación, y para la mejora de sus procesos y organización.
- El establecimiento de un modelo de penalizaciones que relacione el nivel de prestación del servicio con su facturación.
- El establecimiento de indicadores que permitan medir el grado de satisfacción percibida por los usuarios del servicio.

6.2. Características de los indicadores

Los indicadores tendrán las siguientes características:

- **Código**. Identificador único del indicador.
- **Nombre**. Define el objeto de medida del indicador.
- **Descripción**. Descripción del indicador y su objetivo. Se incluyen las restricciones necesarias para llevar a cabo el cálculo del valor del indicador (por ejemplo, restricciones horarias, tipificación de los incidentes, etc.).
- **Categoría**. Agrupa diferentes ANS de un mismo tipo. Por ejemplo: Proyecto, reporting, entre otros.
- **Fórmula de obtención/herramienta**. Fórmula cálculo del valor del indicador de medida, identificando las variables que intervienen en el cálculo (métricas) y, si procede, la referencia a la herramienta que permite la automatización y extracción de los datos.
- **Periodicidad**. Frecuencia de medida del valor del indicador.
- **Umbrales de grado para la definición de los tramos**. Valores que definen el grado de cumplimiento del nivel de servicio exigido. Para cada indicador se definirán 4 umbrales de grado. En función de la banda en que se encuentre el indicador presentará los valores siguientes:



- **Penalización máxima (PPMax).** Determina el valor máximo al cual puede llegar la penalización en el caso de incumplimiento del umbral objetivo definido.

6.3. Grado del indicador

El grado del indicador puede tomar los siguientes valores:

Grado	Valor
1	Deficiente o Inaceptable
2	Insatisfactorio
3	Satisfactorio
4	Excelente

El grado 4 será el nivel objetivo, mientras que el grado 3 será el nivel de cumplimiento mínimo para considerar que el indicador es satisfactorio.

6.4. Cálculo de los indicadores

Para todo indicador se establecen 4 umbrales para definir los tramos lineales que tienen que permitir la obtención del grado asociado.

	Llindar Grau 1	**Llindar Grau 2**	**Llindar Grau 3**	**Llindar Grau 4**
Indicador de mesura	**Valor 1**	**Valor 2**	**Valor 3**	**Valor 4**

Para el valor medido en un indicador (valor indicador), se tendrá que buscar entre qué umbrales se encuentra y aplicar el siguiente procedimiento, teniendo en cuenta si los valores definidos por los umbrales (Valor 1 – Valor 4) son crecientes o decrecientes:

- **valores de umbrales crecientes** (valor Umbral Grado 1 < valor Umbral Grado 4).
    - Si el valor es inferior al umbral 1, el grado será 1.
    - Si el valor es igual o superior al umbral 4, el grado será 4.
    - En el resto de los casos, se aplicará la fórmula de cálculo del grado.

- **valores de umbrales decrecientes** (valor Umbral Grado 1 > valor Umbral Grado 4).
    - Si el valor es superior al umbral 1, el grado será 1.
    - Si el valor es igual o inferior al umbral 4, el grado será 4.
    - En el resto de los casos, se aplicará la fórmula de cálculo del grado.

6.4.1. Fórmula de cálculo del grado

$$Grado = \frac{(Valor\ indicador - Valor\ umbral\ inferior)}{(\text{Valor umbral superior } - \text{Valor umbral inferior})} + Grado\ correspondiente\ al\ umbral\ inferior$$

Al aplicar la fórmula de cálculo del grado, hay que tener en cuenta las siguientes consideraciones:

- Cuando dos o más umbrales toman el mismo valor, el valor del "Grado correspondiente al umbral inferior" corresponde al del umbral coincidente superior.

  Por ejemplo, cuando el Umbral Grado 1 y el Umbral Grado 2 toman el mismo valor, el "Grado correspondiente al umbral inferior" corresponde al del Umbral Grado 2, es decir, toma valor 2.

- Cuando el valor medido por un indicador (valor indicador) coincide con alguno de los valores definidos por los umbrales (Valor 1, Valor 2, Valor 3), se tomará como "Valor umbral inferior" el valor correspondiente al umbral coincidente. Cuando dos o más umbrales toman el mismo valor, se tomará como "Valor umbral inferior" el valor correspondiente al umbral coincidente superior.

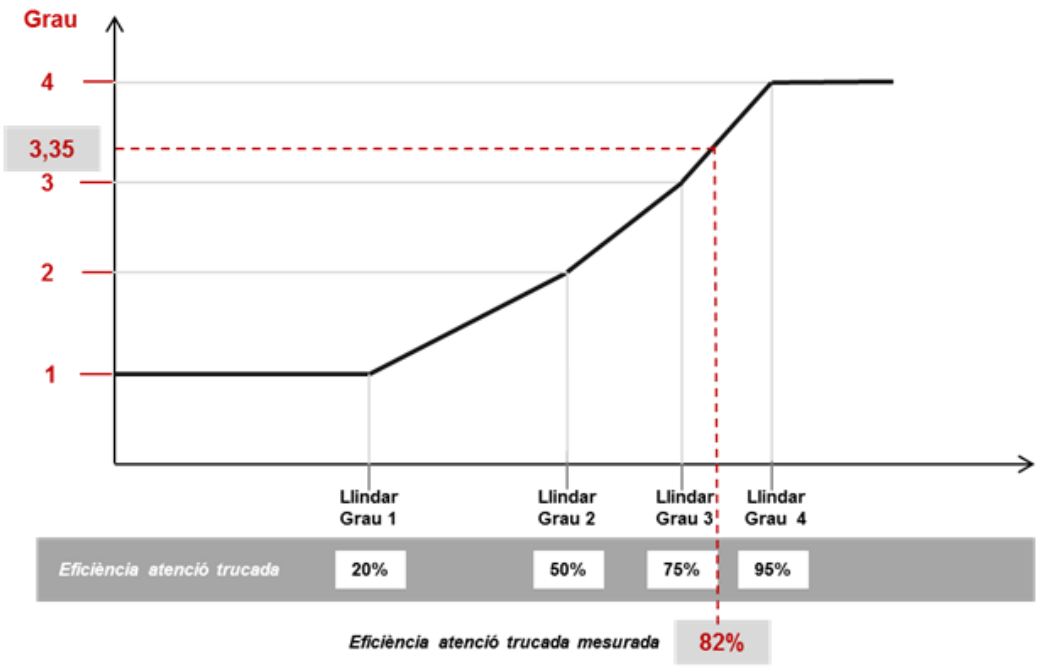
  Por ejemplo, suponiendo los siguientes valores de umbrales: Umbral Grado 1 y el Umbral Grado 2 el mismo valor, 20%, Umbral Grado 3 valor 75% y Umbral Grado 4 valor 95%; cuando el valor medido por el indicador valor 20%, el "Valor umbral inferior" valor 20%, el "Valor umbral superior" valor 75% y el "Grado correspondiente al umbral inferior" valor 2.

6.4.2. Ejemplo de cálculo

Suponemos que tenemos el indicador "Eficiencia atención llamada" que puede tomar valores porcentuales entre 0% y 100% y que el valor objetivo es 95%. Si se han definido los siguientes umbrales:

Umbral Grado	Valor del indicador
1	20%
2	50%
3	75%
4	95%

Si el valor mesurado en un periodo el indicador “Eficiencia atención llamada” ha sido 82%, el grado calculado es: ((82-75)/(95-75))+3=3,35.



Este modelo es dinámico, ya que permite adaptarse en el tiempo a nuevos niveles objetivos y niveles mínimos, sin variar los grados posibles

6.5. Relación de ANS

En el fichero anexo “ANS_EnQGenCat_v.01.xlsx” se encuentran los indicadores definidos para los servicios descritos en este documento. Los indicadores que constan se aplicarán en el cálculo de las penalizaciones por incumplimiento del umbral mínimo requerido como se ha explicado anteriormente.

7. MODELO DE GOBERNANZA

7.1. Objetivo

El modelo de gobernanza TIC de la Generalitat de Catalunya tiene como objetivo gestionar de manera eficiente y eficaz los recursos TIC disponibles, con el fin de garantizar el mejor servicio que dé respuesta a necesidades estratégicas, de seguridad y operativas de los departamentos y entidades.

En concreto este modelo pretende alcanzar los siguientes objetivos estratégicos principales:

- **Calidad**: Garantizar la calidad en la prestación de servicios y la satisfacción de los usuarios, según las necesidades de los diferentes departamentos y entidades de la Generalitat.
- **Eficiencia**: Optimizar el uso de los recursos gracias a la búsqueda de eficiencias, sinergias y optimización.
- **Innovación**: Transformar e innovar a la administración de acuerdo con la estrategia transversal de las TIC de la Generalitat y de cada uno de los departamentos y entidades.
- **Seguridad**: Garantizar que todos los servicios TIC prestados incorporan las medidas de seguridad necesarias de acuerdo con las directrices de la Agencia de Ciberseguridad de Cataluña y los equipos están preparados para hacer frente a posibles incidentes de ciberseguridad.
- **Conocimiento**: Generar conocimiento a partir de la información gestionada con las TIC, para dar respuesta a las necesidades y a la toma de decisiones en el ámbito del negocio de los departamentos y entidades.

7.2. Alcance

El modelo de prestación de servicios TIC está definido como un escenario multi-proveedor con externalización de servicios tecnológicos. El responsable de la estrategia y el Gobierno TIC es el CTTI y el modelo de gobernanza establece el modelo de relación entre los diferentes actores implicados (Generalidad, CTTI, y proveedores). Así pues, este modelo de relación establece las actividades, entradas y salidas de los diferentes comités que lo configuran, así como los mecanismos de seguimiento para asegurar que la gobernanza se lleva a cabo de la manera más eficaz y eficiente posible.

7.3. Modelo de relación

El modelo de relación define las funciones y responsabilidades del proveedor y del CTTI en un marco de actuación común, para asegurar el cumplimiento de las obligaciones de cada una de las partes. Es un marco de relación que permite acordar el contenido y nivel de la prestación de los servicios, así como el seguimiento de la prestación real en los aspectos estratégicos, contractuales, tácticos y operativos.

El adjudicatario puede ampliar, mejorar y detallar, partiendo de las directrices aquí marcadas, la organización propuesta y el esquema específico de la relación con el CTTI, así como los mecanismos de control propios de cada servicio y función transversal. El equipo de trabajo de los proveedores tendrá que disponer del dimensionado, la formación y los medios adecuados para desarrollar las tareas asignadas.

El modelo de relación se sustenta en una estructura de competencias y funciones que recaen sobre un esqueleto de responsables del proveedor, los cuales se relacionarán con el CTTI en base a 3 niveles (estratégico, táctico y operativo).

El proveedor asignará al CTTI a los responsables que sostendrán el Modelo de Relación. El equipo de responsables tendrá que disponer igualmente del dimensionado, la formación y los medios adecuados para desarrollar las funciones y responsabilidades asignadas.

7.3.1. Niveles del modelo de relación

Los niveles funcionales del modelo de relación son el nivel estratégico, el táctico (visión de negocio y visión tecnológica) y el operativo.

Tanto el adjudicatario como el CTTI se comprometen en que las decisiones tomadas en un nivel fluyan al nivel posterior o anterior.

7.3.1.1. Nivel Estratégico

A nivel estratégico, el CTTI y los proveedores tendrán un intercambio de experiencias y visiones sobre el estado del arte de los servicios y las tendencias de evolución tecnológica de estos.

Los asistentes por parte del adjudicatario a los comités de este nivel tendrán capacidad de decisión sobre los compromisos de servicios.

El nivel estratégico, desde la perspectiva del proveedor, es el nivel máximo de seguimiento del contrato y la prestación del servicio. Desde este nivel, se elevará al órgano de contratación las propuestas de actuación en aquellos aspectos que puedan originar la modificación del contrato.

7.3.1.2. Nivel Táctico

En este nivel se hará un seguimiento exhaustivo de la ejecución de los servicios tecnológicos y de negocio y de los contratos y se elevará al nivel estratégico aquellos aspectos que puedan originar la modificación del contrato.

7.3.1.3. Nivel Operativo

Este nivel tiene como objetivo la operación diaria del servicio según los procedimientos desarrollados y tratar las problemáticas específicas que afecten al servicio prestado.

7.3.2. Órganos de Gestión (Comités)

A continuación, se describen la composición de los diferentes comités entre el CTTI y el proveedor, así como otros actores de la Generalitat, y su funcionamiento, para asegurar el cumplimiento de los requerimientos de las condiciones de ejecución de los servicios descritas en este . Estos comités tendrán también como función ejecutar los mecanismos para ajustar estas condiciones de acuerdo con la evolución de las necesidades de servicio.

El licitador tendrá que hacer explícita la estructura y funcionamiento de los Comités de relación y coordinación que sean precisos para mantener una interlocución permanente con los actores involucrados en el proceso.

Si así lo estimara conveniente, el CTTI podrá exigir cambios en la frecuencia de celebración de las reuniones, así como solicitar reuniones extraordinarias de seguimiento.

De forma extraordinaria, y bajo la supervisión del comité de nivel táctico, podrá formarse un equipo de trabajo de carácter temporal con objetivos específicos acordados previamente.

Tanto el proveedor como el CTTI se comprometerán en que las decisiones tomadas en un nivel fluyan al nivel posterior o anterior.

Se describen a continuación los diferentes comités identificados anteriormente con la siguiente estructura a título enunciativo, sin perjuicio que a lo largo de la ejecución del servicio se puedan ajustar las características de cada comité (Participantes, Objetivos, Entradas, Salidas, etc.).

En este sentido, el proveedor tendrá que incorporar a los diferentes comités a las personas responsables de cada ámbito de ejecución en función de los temas específicos a tratar en el comité.

7.3.2.1. Comité Estratégico

Formado por el responsable de la empresa adjudicataria y los representantes que el CTTI determine, los asistentes por parte del proveedor a este comité deberán disponer de capacidad decisoria sobre los compromisos de servicios.

<table>
<tr><th colspan="4">Título</th></tr>
<tr><td colspan="4">Comité Estratégico</td></tr>
<tr><th colspan="2">Participantes mínimos</th><th colspan="2">Objetivos / Temas</th></tr>
<tr><td colspan="2">CTTI</td><td colspan="2" rowspan="8">Marcar las directrices estratégicas del contrato.

Realizar el seguimiento del conjunto de actividades desarrolladas en el periodo, orientado especialmente a la consecución de los objetivos y eficiencias planteadas por el proveedor.

Planificar, priorizar y revisar las iniciativas en curso.

Trasladar las directivas estratégicas al nivel inferior.

Mantener una actitud proactiva en todos los aspectos de la relación, interesándose por el cumplimiento de los ANS e impulsando, dentro de su organización, cualquier medida de la cual pueda resultar una mejora continua de la calidad global del servicio.

Hacer seguimiento del modelo económico.

Revisión y estado de situación de los aspectos más relevantes de seguridad (riesgos, incidentes del periodo, proyectos en curso).

Revisar y proponer las penalizaciones por incumplimiento del servicio y escalarlas en el órgano de contratación.

Planificar, priorizar y revisar las actividades con impacto transversal.

Hacer el seguimiento de las obligaciones contractuales.

Desarrollo de propuestas de innovación en línea con la estrategia transversal del CTTI.

Elevar al órgano de contratación las propuestas de actuación en aquellos aspectos que puedan originar la modificación del contrato.</td></tr>
<tr><td colspan="2">Dirección CTTI

Responsable del contrato (si procede)

Otros asistentes (si procede)</td></tr>
<tr><td colspan="2">Generalitat</td></tr>
<tr><td colspan="2">Responsable Agencia de Ciberseguridad (si procede)</td></tr>
<tr><td colspan="2">Proveedor</td></tr>
<tr><td colspan="2">Responsable de cuenta

Responsable de servicios

Responsables de los ámbitos de ejecución específicos. (si procede)</td></tr>
<tr><th colspan="2">Entradas</th><th colspan="2">Salidas</th></tr>
<tr><td colspan="2">Informes y cuadros de mandos del contrato.

Actos comités ejecutivos.

Decisiones a tomar.</td><td colspan="2">Acta (firmada digitalmente entre las partes)

Decisiones tomadas</td></tr>
</table>

	Propuestas en el Órgano de Contratación
Periodicidad	
- Anual o a petición del CTTI.	

7.3.2.2. Comité Ejecutivo

Formado por el responsable de cuenta y de servicios, así como los representantes que el CTTI determine.

Título	
Comité Ejecutivo	
Participantes mínimos	**Objetivos / Temas**
CTTI Responsable del seguimiento del contrato Responsable del servicio Otros asistentes (si procede) Generalitat Responsable Agencia de Ciberseguridad (si procede) Proveedor Responsable de cuenta Responsables de servicios Responsables de los ámbitos de ejecución específicos (si procede)	Marcar las directrices tácticas del contrato. Realizar el seguimiento del conjunto de actividades desarrolladas en el periodo, orientado especialmente a la consecución de los objetivos y eficiencias planteadas por el proveedor. Revisión y estado de situación de los aspectos más relevantes de seguridad (riesgos, incidentes del periodo, proyectos en curso). Informar y proponer al comité estratégico las posibles modificaciones del contrato que se tengan que llevar a cabo. Realizar el seguimiento y control global de la operación y provisión de los servicios de acuerdo con los acuerdos de niveles de servicio definidos. Revisar y proponer las penalizaciones por incumplimiento del servicio y escalarlas al comité estratégico. Acordar los cuadros de mandos del contrato. Realizar el seguimiento y control global de la operación y provisión de los servicios de acuerdo con los acuerdos de niveles de servicio definidos. Trasladar las directrices tácticas al nivel operativo. Planificar, priorizar y revisar las actividades. Hacer el seguimiento de las obligaciones contractuales y del modelo económico del contrato. Desarrollar propuestas de innovación en línea con la estrategia transversal del CTTI.
Entradas	**Salidas**

- Informes y cuadros de mandos de seguimiento del servicio. - Actos comités operativos. - Actos comités operativos de seguridad. - Decisiones a tomar.	- Acta (firmada digitalmente entre las partes). - Decisiones tomadas. - Propuestas al comité estratégico
Periodicidad	
- Semestral o a petición del CTTI.	

7.3.2.3. Comité Operativo

La periodicidad de este comité se prevé que sea mensual, pero este plazo se podrá modificar de acuerdo con las necesidades del servicio.

Título	
Comité Operativo	
Participantes mínimos	**Objetivos / Temas**
CTTI Responsable de servicio Responsable del seguimiento del contrato (si procede) Otros asistentes (si procede) Proveedor Responsables de servicios Responsables operativos del servicio	Realizar el seguimiento y control global de la operación y provisión de los servicios de acuerdo con los ANS. Planificar, priorizar y revisar las iniciativas en curso. Realizar el seguimiento de la operación diaria del servicio, y verificar la correcta gestión de peticiones, cambios, problemas e incidentes. Desarrollar y mantener los procedimientos operativos necesarios para el correcto funcionamiento de los servicios. Análisis de peticiones y/o situaciones de cambio en los servicios. Escalado de posibles mejoras detectadas en el servicio. Tratamiento de las problemáticas específicas. Desarrollo de propuestas de innovación en línea con la estrategia y necesidad de negocio del departamento o entidad.
Entradas	**Salidas**
Informes operativos de seguimiento del servicio. Análisis y propuestas de mejora. Decisiones a tomar.	Acta (firmada digitalmente entre las partes) Propuestas al comité ejecutivo. Nuevos procedimientos operativos.
Periodicidad	
Trimestral o a petición del CTTI.	

7.3.2.4. Comité Operativo de Seguridad

Este comité operativo transversal de seguridad tendrá una periodicidad cuatrimestral, pero este plazo se podrá modificar de acuerdo con las necesidades del servicio.

<table>
<tr><th colspan="3">Título</th></tr>
<tr><td colspan="3">Comité Operativo de Seguridad</td></tr>
<tr><th>Participantes</th><th colspan="2">Objetivos / Temas</th></tr>
<tr><td>CTTI

Responsable de servicios

Responsable del seguimiento del contrato (si procede)

Otros asistentes (si procede)

Generalitat

Responsable riesgo tecnológico de seguridad de la Agencia de Ciberseguridad

Proveedor

Responsable de seguridad del proveedor (RSP)

Otro personal operativo</td><td colspan="2">Realizar el seguimiento de la operación y gobernanza de la seguridad por parte del proveedor:

Grado de adecuación al modelo de seguridad que tiene que implementar el proveedor para que se adecue al modelo de Ciberseguridad.

Eficiencia en la gestión de vulnerabilidades de los servicios, haciendo foco en las vulnerabilidades críticas.

Excepciones de seguridad: volumen, criticidad, controles compensatorios a aplicar, etc.

Incidentes de seguridad del periodo. Revisión y gestión de mejoras asociadas.

Niveles de Servicio de Seguridad del proveedor (ANS).

Seguimiento del estado de seguridad de los proyectos en curso: evolutivos, correctivos, etc.

Escalado de problemas

Tratamiento de las problemáticas específicas</td></tr>
<tr><th>Entradas</th><th colspan="2">Salidas</th></tr>
<tr><td>Informes de estado de la seguridad.

Análisis y propuestas de mejora.

Decisiones a tomar.</td><td colspan="2">Acta (firmada digitalmente entre las partes)

- Propuestas al comité ejecutivo</td></tr>
<tr><th colspan="3">Periodicidad</th></tr>
<tr><td colspan="3">- Semestral o a petición del CTTI.</td></tr>
</table>

7.3.3. Estructura de responsabilidades

En este apartado se indican los roles que participarán en los diferentes comités con las funciones y responsabilidades específicas por los servicios objeto de esta licitación.

La empresa licitadora tendrá que presentar un esquema organizativo correctamente dimensionado que asegure la cobertura del servicio requerido.

Acto seguido se identifican los roles responsables del proveedor para asegurar el cumplimiento de las condiciones de ejecución.

7.3.3.1. Responsable de cuenta

Esta figura es única por proveedor. Es la figura de referencia todos los contratos entre el CTTI y el proveedor y el último responsable de la prestación del conjunto de servicios y proyectos del proveedor. El responsable de cuenta tiene que tener capacidad decisoria sobre el servicio, especialmente en el caso de las UTE. Esta figura se mantendrá durante toda la vida del contrato o contratos entre el CTTI y el proveedor, en la gestión comercial, durante la provisión del servicio y hasta la devolución de este. Tiene que ser garante de la existencia de los mecanismos de relación en su organización para llevar a cabo los acuerdos tomados entre CTTI y el proveedor. En caso de que se produzcan cambios en el alcance y/o coste de los servicios que impliquen una modificación contractual, es el responsable de vehicularlo.

Entre sus responsabilidades se destacan:

Consolidar y aportar al CTTI las informaciones tanto objetivas como subjetivas; valoradas (información fiable y de calidad y analizada de acuerdo con el conocimiento del modelo) que permitan la toma de decisiones operativas y estratégicas a lo largo de la vida del contrato.

Ser el interlocutor principal con el CTTI en materia jurídico-legal para todos los servicios/contratos prestados por el proveedor. Será el responsable de la formalización de las interpretaciones realizadas con respecto a los contratos vigentes, cuando estas impliquen modificaciones contractuales. Ser el responsable que el CTTI reciba los informes de gestión acordados, tanto con indicadores económico-financieros como de otros, así como de realizar el seguimiento del modelo económico acordado con el proveedor.

Ser el responsable que el proveedor facilite la información relativa al proceso de facturación, según el modelo y formado definido por el CTTI, así como colaborar en el proceso de la conciliación.

7.3.3.2. Responsables de servicios

El proveedor asignará un responsable para cada uno de los servicios prestados teniendo en cuenta los ejes del modelo de relación. Con el fin de garantizar la consecución del objetivo del modelo de disponer de un servicio totalmente alineado a las necesidades de los diferentes departamentos y entidades, en caso de que el servicio requiera incorporar el eje de relación de ámbito departamental del modelo de relación, el proveedor tendrá que asignar un responsable de servicio específicamente a cada departamento o entidad en lo que preste servicio. Tendrá también que asignar un responsable del servicio desde la perspectiva transversal de este. Sus principales responsabilidades son:

La gestión y seguimiento diario del servicio, así como la resolución de conflictos y redimensionado temporal o permanente de este.

Mantenimiento del registro de la evolución del servicio para posteriormente poder elaborar los informes de servicio y justificar el cumplimiento de los ANS.

Seguimiento y control de los recursos asignados a los servicios.

Analizar cualquier desviación y situaciones de gravedad dentro de la calidad, plazos o alcance del servicio.

A nivel transversal, realizar el control de costes, la estimación de esfuerzos y su seguimiento.

A nivel transversal, analizar las modificaciones en alcance y coste del servicio que se puedan derivar e interpretar estas modificaciones respecto de los contratos vigentes. En caso de que no impliquen una modificación contractual, ser el garante de formalizar e implementar internamente a su organización los acuerdos tomados.

Asegurar la buena colaboración entre los diferentes proveedores con quienes se tienen que relacionar con el fin de mejorar el servicio de negocio final.

7.3.3.3. Responsable de seguridad (RSP)

Este responsable es único por proveedor, y es la figura de referencia con respecto a ciberseguridad todos los contratos entre el CTTI y el proveedor. Tiene que liderar y garantizar que los servicios prestados por el proveedor alcanzan los requerimientos de seguridad solicitados. Será responsable de:

Actuar como enlace entre el proveedor y los diferentes agentes implicados (CTTI, Agència de Cibersegurerat, oficina QA de ciberseguridad) cuando se traten temas de seguridad.

Garantizar, liderar e impulsar el cumplimiento del marco normativo de seguridad de la Generalitat de Catalunya dentro de su organización, asegurando la correcta implantación de los niveles de seguridad y sus correspondientes medidas (técnicas, organizativas, y jurídicas); así como las directrices en materia de seguridad definidas por la Agència de Cibersegurerat.

Coordinar reuniones de seguimiento periódicas con CTTI y la Agència de Cibersegurerat para informar del grado de adecuación de los servicios al modelo de seguridad de la Generalitat de Catalunya, identificar los riesgos más relevantes y proponer planos de acción su mitigación.

Que todo el personal de la empresa que prestará servicios al CTTI y la Generalitat, pase por un plan de concienciación y formación en materia de seguridad, focalizándose en el marco normativo de la Generalitat y los procedimientos de seguridad que le sean de aplicación.

Asegurar la información regular en el CTTI, Oficina QA de ciberseguridad y a la Agència de Cibersegurerat según los plazos marcados, de todo el relacionado con la seguridad (incidentes, medidas correctoras, riesgos, nuevos proyectos, iniciativas, etc.).

He de asegurar que todo el personal del proveedor que tenga que tratar datos o sistemas de tratamiento de datos de nivel sensible o superior firmen un Acuerdo de

Confidencialidad Individual. El CTTI y la Agència de Cibersegurerat podrán auditar este aspecto.

Coordinación operativa con el equipo de respuesta a incidentes y con el SOC de la Agencia de Ciberseguridad ante incidentes o posibles amenazas de ciberseguridad (entrega de evidencias la gestión e investigación de incidentes de seguridad, soporte para la aplicación rápida de medidas de protección y contención ante amenazas o ciberincidentes, disponer de información vinculada al dispositivo, etc.).

Utilizar el Portal de Seguridad de forma regular para hacer el seguimiento de toda la información vinculada a la seguridad de los activos de la Generalitat de Catalunya.

Garantizar y liderar dentro de su organización la correcta implantación de los planes de continuidad y disponibilidad acordados con el CTTI y la Agència de Cibersegurerat.

Garantizar la ejecución de pruebas de recuperación de desastres de los servicios objeto del contrato, de forma coordinada con el CTTI y la Agència de Cibersegurerat.

Coordinar todo el ámbito formativo en ciberseguridad, tanto las sesiones formativas que se impartirán junto con la Agència de Cibersegurerat, como las tareas de concienciación/formación que los técnicos tendrán que trasladar a los usuarios finales (recomendaciones, píldoras, vídeos formativos, etc.).

Garantizar la ejecución de pruebas de recuperación de copias de seguridad para validar la correcta ejecución.

Asegurar la información regular según los plazos marcados, del relacionado con la Continuidad y Disponibilidad (incidentes, medidas correctoras, riesgos, nuevos proyectos, iniciativas, etc.

Facilitar los indicadores que se consideren oportunos para garantizar los niveles de seguridad que establezca la Agència de Ciberseguretat y CTTI.