PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS DE ATENCIÓN CENTRALIZADA AL PERSONAL TÉCNICO DEL DEPARTAMENTO DE IT PARA EL INSTITUTO CATALÁN DE NANOCIENCIA Y NANOTECNOLOGÍA (ICN2)

Exp. 2026-15 ICN2

1. INTRODUCCIÓN

La actividad principal del Instituto Catalán de Nanociencia y Nanotecnología, en adelante ICN2, es la prestación de servicios de investigación y docencia. Adicionalmente a esta actividad, también se realiza la gestión de apoyo a otros servicios del entorno científico ubicadas en el ICN2, así como la gestión de los inmuebles e instalaciones del centro.

Los objetivos principales que se pretenden alcanzar con la presente licitación son:

- Asegurar la continuidad y disponibilidad de los servicios de IT en el centro, garantizando el funcionamiento correcto de todas las infraestructuras críticas para las actividades de investigación.
- Ofrecer apoyo especializado 24x7 en los entornos tecnológicos más críticos, permitiendo la investigación sin interrupciones.
- Mejorar la eficiencia operacional del Departamento de IT, liberando recursos internos para tareas de transformación digital e innovación.
- Soporte experto en Microsoft Azure y arquitecturas cloud híbridas.
- Garantizar la seguridad de la información mediante prácticas de ciberseguridad de alto nivel y conformidad con estándares internacionales.
- Facilitar la captura y transferencia de conocimiento mediante documentación exhaustiva y base de datos de conocimiento.
- Asegurar la reversión del servicio en caso de finalización del contrato con la mínima interrupción posible.

Para alcanzar estos objetivos, y dado el crecimiento físico y de actividad del ICN2 durante los últimos años, surge la necesidad de potenciar el apoyo tecnológico a aquellas actividades clave para su correcto funcionamiento.

Actualmente, el ICN2 dispone de un Departamento de IT que facilita la atención centralizada al usuario interno y soporte de sus tecnologías de la información y las comunicaciones, y que permite optimizar los recursos disponibles con la máxima calidad en la atención a los usuarios del centro.

El presente documento es el Pliego de Prescripciones Técnicas para la contratación de servicios de apoyo especialista para el Departamento de IT.

2. PRESUPUESTO DE LA LICITACIÓN Y DURACIÓN DEL CONTRATO

El presupuesto total de la licitación para este servicio será de 290.400,00 € (IVA INCLUIDO), con el siguiente desglose: base imponible: 240.000,00 € + 50.400,00 € (21% IVA).

El importe de la anualidad del contrato es de 48.000,00 euros.

La duración del contrato será de CINCO AÑOS, sin posibilidad de prórrogas. El servicio debe estar operativo desde el 1 de octubre de 2026.

A todos los efectos se entenderá que en las ofertas y en los precios aprobados están incluidos todos los gastos que la empresa adjudicataria debe realizar para el normal cumplimiento de las prestaciones contratadas, como son, los generales, beneficio industrial, salarios, financieros, benéficos, seguros, transportes y desplazamientos, honorarios del personal a su cargo, de comprobación y ensayo, materiales necesarios, tasas y toda clase de tributos, en especial el Impuesto sobre el Valor Añadido (IVA) y cualquier otro que pueda establecerse o modificarse durante la vigencia del contrato, sin que

por tanto puedan ser repercutidos como partida independiente, sin perjuicio de los gastos adicionales e indeterminados económicamente derivados de los Pliegos.

3. OBJETO DEL CONTRATO Y DEFINICIÓN DE ACTIVIDADES

3.1 Objeto general

El objeto de este pliego es la contratación de servicios de soporte integral de infraestructura TIC 24x7 para el ICN2, que incluye:

- Service Desk especializado para atender a personal técnico del ICN2
- Monitorización y gestión proactiva de las infraestructuras TIC en 24x7
- Soporte técnico avanzado (Nivel 2 y 3) en las tecnologías críticas del centro
- Soporte especializado en Microsoft Azure para entornos cloud e híbrido
- Asesoramiento en ciberseguridad e implementación de mejoras continuas
- Mantenimiento preventivo y correctivo de todas las infraestructuras
- Gestión de peticiones de servicio y cambios
- Plan de transición y reversión del servicio
- Software de monitorización (tipo LogicMonitor o equivalente) sin coste adicional

3.2 Alcance tecnológico

El servicio debe cubrir todas las tecnologías, sistemas e infraestructuras TIC actuales del ICN2, así como las que se implementen durante la vigencia del contrato:

3.2.1 Entorno de Redes y Comunicaciones

- Switches Cisco 3560G, 2960, 9200, 9300 y otros del fabricante CISCO
- Core Cisco 9300 y equipamiento de distribución
- Wireless LAN Cisco Meraki
- Telefonía fija a través de Teams

3.2.2 Seguridad de Red y Defensa Perimetral

- Firewall FortiGate 900G (Fortinet)
- Soluciones de seguridad Fortinet (IPS, IDS, Web Filtering, Antivirus)

3.2.3 Virtualización y Computación

- Microsoft Hyper-V en servidores Cisco UCS 5108
- Máquinas virtuales Windows Server 2012/2016/2019/2022
- Máquinas virtuales Linux (CentOS 7, Ubuntu Server)

3.2.4 Microsoft Azure Cloud

- Servidores virtuales (Azure VMs) en varias configuraciones
- Azure App Service y aplicaciones web
- Azure SQL Database y managed databases
- Azure Storage (Blob, Files, Tables)
- Azure Networking (VNet, Gateways, ExpressRoute si aplica)
- Azure Security Center y Defender for Cloud
- Azure Backup y Disaster Recovery
- Microsoft 365 / Office 365 (Exchange Online, Teams, OneDrive, SharePoint Online)

3.2.5 Sistemas de Bases de Datos

- SQL Server 2014 y versiones posteriores
- MySQL Server
- MariaDB (en servidores CentOS 7)

- 3.2.6 Almacenamiento y Backup

- NetApp FAS 2820 (File Sharing)
- NetApp FAS 2820 (Backup)
- IBM Storwize V7000 (VM Storage)
- Cabinas QNAP
- BackupExec 20 y Commvault Metallic

3.2.7 Aplicaciones Corporativas

- Microsoft SCCM (Software Center)
- SharePoint on-premise y/o online
- Solución de seguridad XDR Trend Micro

3.3 Entornos de Servicio Diferenciados

El alcance de los servicios según el horario se define de la siguiente manera:

- Monitorización: Se realizará en modalidad 24x7 para TODA la infraestructura (tanto el entorno crítico como el no crítico).
- Mantenimiento preventivo y correctivo/gestión y resolución de incidencias: La gestión y resolución de incidencias se realizará en modalidad 24x7 exclusivamente para el Entorno Crítico. Para el Entorno No Crítico, el horario de apoyo y resolución será de 8x5.
- Gestión de Peticiones de Servicio: Todas las peticiones (estándar y mayores) se atenderán exclusivamente en horario 8x5, independientemente del entorno afectado."

El servicio debe contemplar la cobertura de dos entornos diferenciados por nivel de criticidad:

ENTORNO CRÍTICO (24x7):

- Sistemas de correo electrónico (Exchange Online)
- Firewall y seguridad perimetral (Fortinet)
- Switches y redes principales (Cisco)
- Storage y virtualización (NetApp, IBM, QNAP, Hyper-V)
- Infraestructura Azure (VMs críticos, databases, backups)
- Sistemas de backup (BackupExec y Metallic)

ENTORNO NO CRÍTICO (8x5):

- Sistemas de productividad secundarios
- Otros sistemas que puedan ser pausados temporalmente

4. SERVICIOS A PRESTAR

- 4.1 Service Desk Especializado (Nivel 1)

4.1.1 Disponibilidad

- Jornada estándar: lunes a jueves de 08:00 a 18:00. viernes de 08:00 a 15:00 por entornos no críticos y 24x7 por entornos críticos

- Fuera de jornada estándar: Activación de guardias por entornos críticos
- Festivos: Cobertura de guardia según calendario laboral del ICN2

4.1.2 Vías de Recepción de Peticiones

- Correo electrónico
- Teléfono
- Portal web (ticketing system)
- Herramienta integrada de gestión de incidentes

4.1.3 Funciones del Service Desk Nivel 1

Recepción y Registro:

- Recepción de todas las peticiones, incidentes y avisos
- Registro completo en el sistema de ticketing
- Categorización automática y asignación de prioridad
- Captación de recepción al demandante en el plazo de 15 minutos

Elección y Diagnóstico:

- Diagnóstico inicial del incidente
- Escalado adecuado a Nivel 2 o fabricante cuando sea necesario

Monitorización de Eventos:

- Gestión de todas las alarmas generadas por sistemas de monitorización
- Creación automática de tickets para eventos críticos
- Respuesta a los eventos dentro de los SLA establecidos

4.2 Monitorización Proactiva 24x7

4.2.1 Alcance de Monitorización

- Disponibilidad de sistemas: Verificación continua de que todos los sistemas están en línea
- Recursos computacionales: CPU, memoria, disco, red (latencia, ancho de banda)
- Aplicaciones críticas: Procesos, servicios, puertos, respuestas de aplicación
- Storage: Capacidad, salud de discos, integridad, RAID status
- Networking: Switches, firewalls, routers, VLANs
- Seguridad: Logs de firewall, intentos de intrusión, vulnerabilidades
- Backup: Estado de los backups, éxito/fracaso, capacidades

4.2.2 Detección y Notificación

- Detección proactiva: Identificación de problemas ANTES que afecten a los usuarios
- Alertas automáticas: Notificación al Service Desk (24x7) de eventos críticos
- Escalado automático: Creación de tickets para eventos críticos
- Captación manual: Verificación de falsas alarmas
- Informes de tendencias: Identificación de patrones y problemas recurrentes

4.2.3 Software de Monitorización Requerido

- Plataforma tipo LogicMonitor o equivalente (Datadog, Dynatrace, Site24x7, PRTG, Zabbix Enterprise, etc.)
- Requisitos mínimos:
- SaaS o hybrid deployment
- Monitorización de más de 500 dispositivos/instancias on-premise y cloud
- Integración completa con Azure

- Monitorización de redes (SNMP, NetFlow)
- APM (Application Performance Monitoring)
- Alertas configurables por severidad
- Dashboards personalizables
- API para integraciones terceras
- Retención de datos mínimo 12 meses
- Incluido sin coste adicional
- Acceso: ICN2 debe tener acceso a dashboards y alertas como mínimo en modo lectura
- Informes mensuales: Dashboard de monitorización resumido

4.2.4 Horario de Monitorización

Monitorización 24x7 completa para TODOS los entornos (tanto críticos como no críticos)

4.3 Apoyo Técnico Avanzado Nivel 2 y 3

4.3.1 Nivel 2: Equipo de Técnicos e Ingenieros Especialistas

El adjudicatario debe disponer de equipo de técnicos especializados en las siguientes áreas:

Área Networking y Comunicaciones:
- Experto en Cisco (switches, core, routing, VLANs)
- Experto en Cisco Meraki (WLAN, gestión centralizada)
- Experto en VoIP (Teams)
- Especialista en redes: troubleshooting, optimización, seguridad

Área Seguridad y Firewall:
- Experto Fortinet FortiGate y ecosistema Fortinet
- Especialista en seguridad perimetral, políticas, VPNs
- Especialista en ciberseguridad (SOC, intrusion detection, etc.)

Área Virtualización y Hypervisores:
- Experto en Microsoft Hyper-V
- Especialista en gestión de máquinas virtuales, clustering, high availability
- Especialista en rendimiento y optimización

Área Microsoft Azure:
- Especialista Azure Infrastructure (VMs, networking, storage)
- Especialista Azure Database y data services
- Especialista Azure Security y Compliance
- Especialista en arquitecturas híbridas on-premise/Azure

Área Almacenamiento y Backup:
- Expert NetApp (FAS, configuración, replicación)
- Expert IBM Storage
- Experto BackupExec, Metallic y estrategias de backup/restore
- Especialista en disaster recovery

Área Bases de Datos:
- Expert SQL Server (administración, optimización, seguridad, backups)
- Experto MySQL/MariaDB
- Especialista en tuning de bases de datos, indexing, queries

Área Aplicaciones Corporativas:
- Expert SharePoint (on-premise y online)
- Especialista en SCCM

Área Sistemas Operativos:
- Expert Windows Server (2012/2016/2019/2022)
- Expert Linux/CentOS, Ubuntu Server
- Especialista en patching, updates, seguridad de OS

4.3.2 Funciones Nivel 2

Resolución Técnica Avanzada:
- Diagnóstico profundo de problemas complejos
- Resolución de incidencias
- Realización de cambios estructurales y configuraciones

Apoyo Preventivo:
- Revisión periódica de logs y parámetros de configuración
- Identificación de problemas potenciales
- Realización de mantenimientos planificados
- Recomendaciones de mejora y optimización

Gestión de Cambios:
- Planificación y ejecución de cambios estructurales
- Testing en entornos pre-producción
- Coordinación de ventanas de mantenimiento
- Plan de rollback en caso de problemas

Documentación:
- Actualización de base de datos de conocimiento
- Creación de procedimientos de resolución
- Documentación de configuraciones

4.3.3 Nivel 3: Escalado en Fabricantes

Para problemas de complejidad muy elevada o requeridos por garantías de fabricante:

Actividades Nivel 3:
- Apertura de tickets con fabricantes (Cisco, Fortinet, Microsoft, NetApp, Veritas, Metallic, etc.)
- Seguimiento del escalado con soporte de fabricante
- Coordinación entre adjudicatario, fabricante e ICN2
- Participación en conferencias telefónicas de apoyo

Requisitos Nivel 3:
- Respuesta inicial dentro de SLA
- Acceso a partners/resellers de los fabricantes con altos niveles de partnership
- Relación establecida con support teams de fabricantes
- Gestión proactiva del escalado para evitar demoras

4.4 Soporte Especializado en Microsoft Azure

Dado el rol estratégico de Azure en la transformación digital del ICN2, este servicio merece cobertura específica:

- 4.4.1 Áreas de Expertise Azure

- Microsoft Azure Infrastructure (IaaS)
- Microsoft Azure App Services (PaaS)
- Microsoft Azure Databases
- Microsoft Azure Networking y conectividad
- Microsoft Azure Security y Compliance
- Microsoft 365
- Escenarios híbridos (on-premise/Azure)
- Optimización de costes

4.4.2 Responsabilidades Apoyo Azure

- Monitorización 24x7 de recursos Azure críticos
- Recomendación proactiva de optimización de costes
- Soporte para deployments, updates, patches
- Scaling y autoscaling management
- Disaster recovery y business continuity
- Performance tuning y optimizaciones
- Recomendaciones de seguridad
- Compliance monitoring
- Soporte de acceso a Microsoft Support (en coordinación con ICN2 si requiere)

4.5 Mantenimiento Preventivo y Correctivo

4.5.1 Mantenimiento Preventivo

Mensualmente:

- Revisión de logs de todos los sistemas críticos.
- Revisión de capacidades (disco, memoria, BD) y alertas de proximidad a los límites.
- Informes con recomendaciones de mejora continua.

Trimestralmente:

- Pruebas de restauración aleatorias (mínimo una vez cada 3 meses). El adjudicatario debe incluir en estas pruebas de restauración elementos de los diferentes tipos de backups que se hacen (archivos, 365, servidores, etc).
- Tras cada prueba de restauración, el adjudicatario deberá entregar un informe detallado con los resultados, tiempo de restauración y posibles errores detectados.
- Mantenimiento de bases de datos (reconstrucción de índices, actualización de estadísticas, purga de logs).

Semestralmente:

- Patching e instalación de security updates en Sistemas Operativos y aplicaciones.
- Auditoría de permisos y accesos a sistemas.
- Revisión profunda de políticas de firewall y seguridad y recomendaciones de mejora.
- Revisión de configuraciones estructurales para detectar desviaciones.

4.5.2 Mantenimiento Correctivo

Resolución de Incidencias:
- Soporte 24x7 para incidencias
- Respuesta garantizada dentro de los SLA
- Troubleshooting metodológico
- Implementación de soluciones permanentes (no sólo workarounds)
- Root cause analysis post-incident

Capacidades de Restauración:
- Recovery de datos corruptos
- Restore de backups
- Rebuild de sistemas si necesario
- Testing de restauraciones

4.6 Gestión de Peticiones de Servicio

4.6.1 Tipos de Peticiones

Peticiones Estándar:
- Cambios de configuración menores
- Cambios de política de seguridad
- Nuevas VM o elementos de Azure

Peticiones de Servicio Mayores:
- Actualizaciones mayores de sistemas (cambios de versiones de sistemas operativos de servidores, por ejemplo)
- Reconfiguraciones de red

En el caso de peticiones de servicio mayores, se evaluará con el adjudicatario la viabilidad de ejecutar la petición. Para aquellas actuaciones que se consideren fuera de este servicio, se hará uso de la bolsa de horas extraordinarias ofertada por el licitador (según el Criterio A.2.4 del Anexo 3), siempre que el adjudicatario haya puesto a disposición esta bolsa y haya saldo de horas suficiente. La ejecución mediante esta bolsa de horas requerirá, en todo caso, la validación previa del Responsable de IT del ICN2.

4.6.2 Informes de Peticiones

- Estadísticas mensuales: Número de peticiones, tipos, duración media
- Trending: Análisis de patrones de peticiones
- Recomendaciones: Mejoras sugeridas basadas en demanda

4.6.3 Horario de Ejecución

Todas las peticiones de servicio descritas en este apartado serán atendidas y ejecutadas exclusivamente en horario estándar (8x5), excepto si afectan a servicios críticos e implican downtime o degradación del servicio. En este caso, se programará la intervención fuera de horas para que la afectación sea mínima.

4.7 Software de Monitorización

4.7.1 Requisitos

El adjudicatario debe proporcionar una plataforma de monitorización de la infraestructura on-premise y cloud. Actualmente usamos LogicMonitor, proporcionada por el actual adjudicatario.

En este caso hay dos escenarios:

- Una herramienta proporcionada por el licitador donde el ICN2 tenga acceso durante la duración del contrato. En este caso debe ser sin coste alguno para el ICN2.
- Una herramienta comercial/open source instalada y configurada por el licitador en servidores propios del ICN2. En este caso, la instalación y configuración de la herramienta y de la infraestructura necesaria no tiene ningún coste para el ICN2. El coste recurrente del servidor en Azure y el coste de la herramienta (en caso de ser comercial) sí es responsabilidad del ICN2. En este segundo escenario, esta herramienta sí quedará para siempre en los servidores del ICN2 y tendrá los derechos de uso.

En cualquier caso, la decisión final de qué herramienta se utilizará es del ICN2.

4.7.2 Plataformas Sugeridas

La plataforma de monitorización debe ser alguna de estas o similares: Datadog, Dynatrace, Site24x7, PRTG Network Monitor, Zabbix Enterprise, Elastic Stack + Observability

4.7.3 Capacidades Requeridas

La plataforma debe tener:

- Monitorización de 500+ dispositivos/instancias sin incremento de coste
- Integración completa con Microsoft Azure
- Integración con Cisco, Fortinet, NetApp
- Monitorización de redes (SNMP, NetFlow, sFlow)
- APM (Application Performance Monitoring)
- Alertas configurables por múltiples canales (email, SMS)
- Dashboards personalizables para roles diferentes
- Informes automáticos (daily, weekly, monthly)
- API REST completa para integraciones terceras
- Retención de datos mínimo 12 meses
- High availability del servicio de monitorización (SLA 99.9% mínimo), sin tener en cuenta paradas planificadas

4.7.4 Responsabilidades del Adjudicatario

- Provisioning y configuración de la plataforma
- Integración con sistemas ICN2 (redes, Azure, databases, etc.)
- Configuración de agentes/collectores en dispositivos monitorizados
- Creación de dashboards personalizados para ICN2
- Configuración de alertas según severidad y criticidad
- Formación inicial al personal del ICN2 (mínimo 4 horas)
- Support y mantenimiento de la plataforma
- Backup de configuraciones y datos de monitorización
- Mejoras y optimizaciones mensuales

4.7.5 Acceso y Responsabilidades del ICN2

- Acceso completo a los dashboards y datos
- Capacidad de crear custom views dentro de la plataforma
- Acceso a APIs para integraciones
- Responsabilidad de políticas de escalado de notificaciones (ICN2 define cuándo notificar a quién)
- Responsabilidad de políticas de retención de datos (dentro de los límites técnicos)

4.8 Plan de Puesta en Marcha

4.8.1 Fases del Plan

Fase 0: Pre-planificación (1-2 semanas previas)
- Reunión inicial con ICN2
- Definición de scope final
- Asignación de recursos
- Planificación de calendario

Fase 1: Elaboración del Plan (1-2 semanas)
- Documento detallado con:
- Organización del adjudicatario
- Modelo de relación con ICN2
- Procedimientos de explotación
- Planes de contingencia
- Responsabilidades y escalado
- Cronograma
- Aprobación por parte del ICN2

Fase 2: Setup Técnico (1-2 semanas)
- Configuración de los sistemas de ticketing
- Setup de monitorización
- Configuración de comunicaciones
- Setup del software de monitorización
- Testing de procedimientos
- Preparación de base de datos de conocimiento

Fase 3: Captura de Conocimiento (2-3 semanas)
- Documentación de configuraciones actuales
- Procedimientos de troubleshooting
- Contactos de fabricantes
- Documentación arquitectura
- Procesos operacionales
- Transferencia de conocimiento: Base de datos de conocimiento poblada con casos

Fase 4: Piloto y Testing (1 semana)
- Gestión de incidentes en modo piloto
- Facturación de SLA
- Testing de escalados
- Facturación de monitorización
- Prove-out de procedimientos

Fase 5: Go-Live (1 día)
- Activación formal del servicio
- Handover oficial
- Transición de todas las responsabilidades

4.8.2 Responsabilidades

- Requisito: Coordinar todas las fases, proporcionar recursos
- ICN2: Facilitar acceso, proporcionar información, participar en reuniones
- Ambos: Resolución rápida de bloqueos

4.9 Plan de Transición/Reversión del Servicio

En caso de finalización del contrato (no renovación, cambio de proveedor, etc.), el adjudicatario debe garantizar la reversión sin impacto operacional.

4.9.1 Actividades de Reversión

Documentación:
- Entrega de toda la documentación de sistemas
- Configuraciones actuales (exportadas)
- Procedimientos de troubleshooting
- Contactos de fabricantes y soportes

Transferencia de Conocimiento:
- Sesiones de formación
- Personal de la nueva empresa o ICN2 formado completamente
- Q&A periodo post-transición

Extracción de Datos:
- Exportación de base de datos de conocimiento (formato open si posible)
- Plan de setup para nuevo proveedor

Superposición:
- Periodo de mínimo 30 días de cobertura simultánea (ambos proveedores activos)
- Apoyo al nuevo proveedor durante transición
- Verificación de que todo funciona con nueva estructura
- Soporte de escalado para problemas detectados en transición

Horario de Ventanas:
- Transición planificada durante horario laboral estándar
- Máxima protección de servicios críticos durante transición
- Plan de rollback si calés

4.10 Control operativo y procedimiento de autorización

Todas las actuaciones realizadas por la empresa adjudicataria sobre la infraestructura del ICN2 (gestión de incidencias, ejecución de peticiones de servicio o cambios) requerirán la validación previa del Departamento de IT.

Este control se articulará bajo las siguientes premisas:

- Autorización previa: Como norma general, ninguna intervención podrá ser ejecutada sin el visto bueno expreso del Responsable de IT del ICN2 o la persona en quien delegue. Cualquier excepción a esta norma deberá ser pactada y autorizada previamente por escrito.

- Protocolo de comunicación 24x7: En caso de incidencias detectadas fuera del horario laboral estándar (modalidad 24x7), el Service Desk del adjudicatario tendrá la obligación de contactar inmediatamente con el Responsable de IT del ICN2. En esta comunicación se deberá informar detalladamente de la naturaleza del incidente y de la propuesta de actuación.

- Capacidad de decisión: Corresponde exclusivamente al Responsable de IT del ICN2 decidir el procedimiento a seguir, incluyendo la activación de los equipos de guardia, la ejecución inmediata de medidas correctoras o la posposición de la actuación en el horario 8x5.

5. ACUERDOS DE NIVEL DE SERVICIO (SLA)

Los tiempos de resolución de los SLA que se detallarán a continuación se aplican exclusivamente a Incidencias. Las Peticiones de Servicio tendrán un tiempo de respuesta de 24h laborables, y su tiempo de resolución se pactará según la complejidad, quedando fuera de las penalizaciones automáticas por interrupción del servicio.

5.1 Definición de Criticidad

Entorno CRÍTICO (Respuesta y soporte 24x7)
- Correo electrónico: Exchange Online
- Firewall y seguridad: FortiGate
- Switches y core: Cisco
- Storage crítico: NetApp, IBM Storwize
- Virtualización: Hyper-V entorno crítico
- Azure: VMs, databases, aplicaciones críticas
- Backup: BackupExec, Metallic
- Aplicaciones corporativas: VMs donde está instalado SAP y los diferentes AVD y DBs

Entorno NO CRÍTICO (Respuesta 8x5)
- Aplicaciones corporativas: SCCM
- Servicios no críticos: Segunda red, aplicaciones de productividad
- Servidores desarrollo/test

5.2 Tiempo de Respuesta y Resolución

Para Entorno CRÍTICO:

Severidad	Descripción	Respuesta	Resolución
CRÍTICA (P1)	Sistema completamente caído, impacto total operaciones	1 hora	4 horas
ALTA (P2)	Sistema degradado, algunas	2 horas	8 horas

	funcionalidades no disponibles		
MEDIA (P3)	Funcionalidad limitada, workaround disponible	8 horas	24 horas
BAJA (P4)	Problema menor, sin impacto significativo	16 horas	7 días

Para Entorno NO CRÍTICO:

Severidad	Descripción	Respuesta	Resolución
CRÍTICA (P1)	Sistema completamente caído	4 horas	24 horas
ALTA (P2)	Funcionalidad significativamente limitada	8 horas	48 horas
MEDIA (P3)	Funcionalidad limitada	24 horas	5 días
BAJA (P4)	Problema menor	5 días	10 días

En tickets críticos (P1) y altos (P2) de entorno crítico, las horas son en 24x7. El resto de tickets de entorno crítico y todos los tickets de entorno no crítico están en 8x5.

5.3 Calidad de Servicio del Service Desk

- Tickets resueltos dentro de SLA: Mínimo 90% de tickets cumple los SLA de tiempo

5.4 Monitorización e informes de SLA

- Dashboards mensuales: Informes de SLA compliance
- Reuniones mensuales: Presentación de resultados al responsable de IT del ICN2
- Análisis de desviaciones: Para cualquier incumplimiento, análisis de causa y plan de corrección
- Plan de mejora: Si SLA no se cumple 2 meses seguidos, plan de mejora documentado

6. EQUIPO DE TRABAJO

6.1 Estructura Requerida

La empresa adjudicataria debe disponer de la estructura de personal siguiente como MÍNIMO:

6.1.1 Responsable de Servicio

- Perfil: Ingeniero de telecomunicaciones, ingeniero informático, o similar
- Certificaciones requeridas:
- ITIL v3, v4 Foundation o superior
- PMP, PRINCE2, o Agile (Project Management)
- Certificación de manufacturero (Cisco, Microsoft, Fortinet, o NetApp)
- Experiencia mínima: 5+ años en tareas similares (gestión de servicios TIC, NOC, SOC, o soporte 24x7)
- Idioma: Catalán, Castellano

- Responsabilidades:
- Relación directa con ICN2
- Escalado final de problemas críticos
- Reuniones mensuales
- Informes

6.1.2 Equipo de Service Desk

Composición mínima:
- Personal suficiente para atender las peticiones del ICN2 tanto en horario laboral como fuera de horario

Requisitos por persona:
- Experiencia en IT Support o similar
- Conocimiento de ticketing systems, ITIL basics
- Habilidades de comunicación (técnico y no-técnico)

6.1.3 Equipo Nivel 2: Especialistas por Tecnología

La empresa debe disponer de personal especializado en CADA una de las siguientes áreas (mínimo 1 por área, si un técnico es especialista en varias áreas también es válido):

Especialistas Requeridos:
- Especialista Networking/Cisco (Switches, Core, VLAN, Routing)
- Especialista Wireless/Meraki (WLAN, movilidad)
- Especialista VoIP/Telefonía (Teams)
- Especialista Firewall/Fortinet (FortiGate, seguridad perimetral)
- Especialista Ciberseguridad (Policías, IDS/IPS, threat detection, SOC)
- Especialista Hyper-V/Virtualización (VMs, clustering, HA)
- Especialista Microsoft Azure (VM, databases, networking, security)
- Especialista NetApp Storage (FAS, replicación, snapshots)
- Especialista IBM Storage
- Especialista Backup (BackupExec, Metallic)
- Especialista SQL Server (Bases de datos, tuning, backups)
- Especialista Linux/OS (CentOS, Ubuntu, patch management)
- Especialista Aplicaciones Corporativas (SharePoint, SCCM)

Requisitos por Especialista:
- Experiencia mínima 3+ años en especialidad concreta
- Certificación de manufacturero o relevante
- Habilidades de troubleshooting avanzadas
- Capacidades de formación y documentación

7. DOCUMENTACIÓN REQUERIDA

7.1 Plan de Puesta en Marcha

La documentación indicada será requerida a la empresa preadjudicataria del contrato en la fase de preadjudicación, de acuerdo con lo dispuesto en la cláusula 16 del PCP.

Objetivo: Garantizar que el servicio esté 100% operativo en aproximadamente 6-8 semanas con transferencia completa de conocimiento.

Contenidos obligatorios:

- Cronograma detallado por semanas mostrando cada fase (preparación, configuración, formación, testing, go-live)
- Responsabilidades claras de cada parte (ICN2 vs) con contactos específicos
- Recursos humanos asignados con nombres, roles y horas dedicadas
- Principales riesgos identificados (retrasos de acceso, problemas de conocimiento) con plan de contingencia
- 5 puntos de control con fechas concretas y firma de aprobación
- Documento de handover final con checklist completo

7.2 Documentación técnica de recuperación

- Manual de Recuperación Técnica (Disaster Recovery Playbook), que incluirá los pasos técnicos para restaurar los servicios críticos en caso de desastre, basándose en las herramientas existentes

- 7.3 Manual de Operaciones

Procedimientos para:
- Escalado de incidentes
- Mantenimientos planificados
- Recovery procedures
- Contact trees

7.4 Plan de Reversión

Documento en caso de finalización del servicio.

8. INFORMES

8.1 Informe Mensual

- SLA Compliance: % de tickets dentro de SLA por severidad
- Incident Statistics: Número de tickets por tipo, tiempo medio resolución
- Availability: Uptime de servicios críticos, análisis de incidentes
- Performance: Trends, incidencias recurrentes
- Recomendaciones: Mejoras sugeridas

8.2 Informe Trimestral

- Análisis profundo: Trends a más largo plazo
- Capacity Planning: Proyecciones de crecimiento
- Security: Resumen de alertas de seguridad, vulnerabilidades detectadas
- Optimización de costes: Recomendaciones de ahorro de costes

8.3 Reuniones Mensuales

- Presentación de informes

- Q&A y discusión de incidencias
- Planificación de mantenimientos
- Escalados de problemas recurrentes
- Action items para los próximos meses

9. OBLIGACIONES DEL ADJUDICATARIO

9.1 Obligaciones de Servicio

- Cumplimiento de los SLA definidos
- Disponibilidad 24x7 por entornos críticos
- Respuesta dentro de tiempos especificados
- Mantener bases de datos de conocimiento actualizada
- Proporcionar software de monitorización sin coste adicional
- Mantener confidencialidad
- Cumplir con leyes y regulaciones aplicables (GDPR, etc.)
- Garantizar que la totalidad de los servicios de soporte, atención técnica, documentación e informes se presten y realicen, como mínimo, en castellano

9.2 Obligaciones de Personal

- Mantener equipo multidisciplinario
- Formar personal en procedimientos ICN2
- Mantener certificaciones vigentes
- Notificar cambios de personal

9.3 Obligaciones Administrativas

- Emitir facturas mensuales
- Proporcionar informes mensuales
- Participar en reuniones mensuales
- Documentar todas las incidencias resueltas
- Proporcionar acceso a dashboards de monitorización

9.4 Obligaciones de Transición

- Plan de reversión documentado
- Transferencia de conocimiento suficiente
- Apoyo durante período de transición
- Disponibilidad de backups

10. VOLUMETRÍA DEL ICN2

A continuación, se detalla la volumetría del ICN2 de los últimos años:

Incidencias:

Categoría	2023	2024	2025	Total
Networking	7	7	89	103
Cloud/Azure	2	4	85	91
Otros	6	4	79	89
Monitorización/Alertas	10	42	14	66
Backup	8	29	24	61
Sistemas	8	11	12	31
Seguridad	6	11	7	24
Comunicaciones	6	5	4	15
Aplicaciones	4	5	4	13
Almacenamiento	2	2	2	6
TOTAL	**59**	**120**	**320**	**499**

Hay que tener en cuenta que, debido a la migración de servidores a Azure y la implantación del sistema de monitorización de la actual empresa, el volumen de tickets en 2025 es superior al habitual.

Peticiones:

Categoría	Número de Peticiones
Seguridad	37
Backup	29
Otros	29
Cloud/Azure	24
Networking	22
Almacenamiento	14
Sistemas	12
Comunicaciones	6
Aplicaciones	2
TOTAL	**175**

11.LUGAR DE EJECUCIÓN

La ejecución del contrato y la prestación de los servicios descritos en este pliego se realizará de manera remota por defecto. Para garantizar la viabilidad operativa, la agilidad en los desplazamientos y la correcta cobertura del servicio, la empresa adjudicataria deberá contar con presencia física (oficinas, personal técnico y recursos operativos) en la provincia de Barcelona durante toda la vigencia del contrato. El adjudicatario estará obligado a desplazar personal técnico presencialmente a las instalaciones del ICN2 (Edificio ICN2) de forma inmediata y sin ningún coste adicional cuando una incidencia, petición o intervención técnica requiera indispensablemente actuación física sobre la infraestructura, siempre cumpliendo con los SLAs establecidos.

12. INFORMACIÓN ADICIONAL:

Se podrá solicitar información adicional mediante el envío de un e-mail a la siguiente dirección: contracts@icn2.cat

En Bellaterra a 8 de junio de 2026

Javiér Dameá
L1-L2 Helpdesk support and Intranet Administrator