Pliego de prescripciones técnicas que regulan la renovación del equipamiento de red y de las instalaciones técnicas del centro de procesamiento de datos (actuación que forma parte de la inversión 2 “Reforzamiento de las capacidades, infraestructuras y equipamientos de los agentes del SECTI” del componente 17 del PRTR).

Barcelona, en la fecha de la firma

Validado por,	Aprovado por,

1. Antecedentes

El Consorcio de Servicios Universitarios de Catalunya (CSUC) tiene una larga tradición en la prestación de servicios de computación de altas prestaciones a la comunidad investigadora. Este servicio tiene como objetivo mejorar la eficiencia de todo el sistema, permitiendo a los grupos de investigación disponer de un hardware de alto rendimiento, gestionado por un equipo de soporte experto y que se mantiene actualizado con las últimas tecnologías disponibles en el mercado.

Todos estos servicios se apoyan en la infraestructura tecnológica disponible en el CSUC. En cuanto a la arquitectura de servidores, esta está orientada a la nube y se basa en un diseño de abstracción en tres capas: virtualización, almacenamiento y hardware.

Este modelo proporciona una arquitectura sólida que permite entornos complejos, de gran volumen, flexibles y redundantes; así como una base tecnológica homogénea y, por tanto, eficiente y sostenible. Además, permite una evolución continua que garantiza la calidad y disponibilidad de los servicios.

2. Objetivo y alcance del proyecto

De acuerdo con los motivos expuestos en la sección anterior, este proyecto tiene como objetivo la renovación y mejora del equipamiento de red y de las instalaciones técnicas del centro de procesamiento de datos (CPD). Esta actuación se articula en tres líneas principales:

- La renovación de los cortafuegos perimetrales, asegurando la continuidad de servicios existentes como la autenticación multifactor (MFA) y el WAF.
- La renovación de la red del CPD, manteniendo parte del equipamiento actual, como los sistemas WAF y los balanceadores de carga.
- La renovación, ampliación y mejora de las infraestructuras técnicas del CPD para garantizar una operatividad óptima y una mayor eficiencia energética y funcional.

El procedimiento de licitación se divide en tres lotes diferenciados:

- Lote 1: Renovación de los cortafuegos perimetrales, asegurando la continuidad de servicios existentes como la autenticación multifactor (MFA) y el WAF.
- Lote 2: Renovación de la red del CPD con reutilización parcial del equipamiento existente, como los WAF y los balanceadores y conmutadores de núcleo modulares de alto rendimiento.
- Lote 3: Renovación, ampliación y mejora de las instalaciones técnicas del CPD, incluyendo adecuaciones que permitan soportar las nuevas exigencias tecnológicas y mejorar la eficiencia energética.

3. Características técnicas del equipamiento

En esta sección se describen, en primer lugar, los requisitos mínimos específicos que debe cumplir el equipamiento indicado en cada uno de los siguientes lotes:

- Lote 1: Renovación del sistema de cortafuegos perimetrales, asegurando la continuidad de servicios existentes como la autenticación multifactor (MFA) y el WAF.
- Lote 2: Renovación del equipamiento de conmutación y encaminamiento de la red del centro de procesamiento de datos, red de gestión fuera de banda y red interna.
- Lote 3: Renovación, ampliación y mejora de las instalaciones técnicas del CPD, incluyendo adecuaciones que permitan soportar las nuevas exigencias tecnológicas y mejorar la eficiencia energética.

En segundo lugar, se detallan las condiciones de instalación y configuración de los equipos, la garantía de soporte y documentación, los contenidos mínimos para el plan de formación y, a continuación, la política de crecimiento junto con las mejoras adicionales que los licitadores pueden ofrecer.

3.1. Requisitos específicos del equipamiento del lote 1

El objetivo de este lote es el suministro de una solución para la renovación del equipamiento de cortafuegos, con un sistema de autenticación multifactor (MFA) para la capa de VPN, que garantice un rendimiento óptimo y seguro de los nuevos servicios de datos en el CSUC.

Las funcionalidades y los requisitos mínimos solicitados para los equipos de cortafuegos son los siguientes:

- Los equipos de cortafuegos deben ser en formato *appliance* de un único fabricante, quedando excluidos los servidores de propósito general y las máquinas virtuales. Deben poder instalarse en un bastidor estándar de 19".
- La solución del equipamiento de cortafuegos debe estar compuesta por dos equipos físicos de idénticas características, redundados y en alta disponibilidad (*HA*, *High Availability*). Deben permitir operar en modo *HA activo-activo* y *activo-pasivo*. En caso de activar sistemas virtuales en el equipamiento físico suministrado, estos podrán funcionar en cualquiera de los dos nodos, de forma que se consiga un modo activo-activo.
    - La transferencia del servicio de un equipo al otro debe poder realizarse sin interrupciones, sin pérdida de conexiones TCP ni parada del servicio.
    - Las configuraciones deben sincronizarse automáticamente entre ambos equipos.
    - En caso de que se requieran licencias o suscripciones para activar la alta disponibilidad, estas deberán estar incluidas en la propuesta durante toda la duración del contrato.
- La solución debe incluir funcionalidades de control de aplicaciones, IPS, antimalware con Cloud Sandbox incluido, filtro web, filtro DNS, antispam, protección antiDoS y

firewall de aplicaciones web (WAF). Todas estas funcionalidades deben estar licenciadas durante toda la duración del contrato.

- Ambos equipos deben disponer de la funcionalidad de cortafuegos virtuales para poder crear entornos completamente diferenciados. Deben incluir, como mínimo, 10 cortafuegos virtuales por cada equipo.
- Debe tener capacidad para, como mínimo, 10.000 políticas de cortafuegos.
- La solución de seguridad debe permitir diferentes modos de funcionamiento, pudiendo combinarse entre los distintos cortafuegos virtuales:
    - Modo transparente
    - Modo *routed*
    - Modo *sniffer*
- Los equipos de cortafuegos deben contar con hardware específico (tipo ASIC) para garantizar el rendimiento requerido; en detalle, deben disponer de un hardware específico para analizar el tráfico a nivel 4 y otro completamente distinto para el nivel 7, asegurando una baja latencia.
- Los cortafuegos deben ser capaces de gestionar hasta 8 millones de sesiones concurrentes, así como un mínimo de 450.000 nuevas sesiones por segundo.
- Deben disponer, como mínimo, del siguiente rendimiento:
    - Rendimiento Firewall: 36 / 36 / 20 Gbps por paquetes de 1.518, 512 y 64 bytes en IPv4.
    - Rendimiento IPS: mínimo 10 Gbps para tráfico Enterprise MIX.
    - Rendimiento NGFW (IPS y control de aplicaciones): mínimo 10 Gbps para tráfico Enterprise MIX.
    - Rendimiento con Threat Protection (IPS, control de aplicaciones y motor antimalware activo): mínimo 8 Gbps para tráfico Enterprise MIX.
    - Rendimiento para tráfico IPSEC VPN (512 bytes): mínimo de 20 Gbps.
    - Rendimiento para tráfico SSL VPN: mínimo de 8 Gbps.
- Debe disponer del siguiente número mínimo de puertos:
    - 1 puerto de consola.
    - 1 puerto USB 3.0 para la conexión de módem 3G/4G y/o *pendrive*. Este puerto debe permitir la instalación desatendida del *firmware* y la aplicación de configuración durante el arranque del equipo, con el fin de ejecutar tareas automáticas de instalación y sustitución del equipamiento.
- Cada uno de los equipos de cortafuegos debe disponer de:
    - 4 x 25GE/10 GE SFP28/SFP+
    - 4 x 10GE/GE SFP+/SFP
    - 8 x GE SFP
    - 16 x GE RJ45
    - 1 puerto HA dedicado
    - 1 puerto de gestión dedicado
    - Disco duro de hasta 480 GB SSD
    - Transceptores para ambos extremos de la conexión
    - Consumo eléctrico inferior a 265 W con todos los puertos ocupados
    - Fuente de alimentación doble

- En caso de que el equipamiento permita ampliaciones modulares de interfaces, será necesario que todos los módulos de ampliación estén equipados con interfaces, como mínimo, de las mismas velocidades que se solicitan para los puertos mínimos obligatorios.
- En caso de que el equipo permita ampliaciones de memoria RAM y disco duro, el *appliance* deberá estar equipado con la máxima capacidad de RAM y de disco soportada por el fabricante.
- Capacidad de gestión de los equipos mediante acceso vía web (https), prescindiendo de interfaces basadas en Java, y terminal (ssh) para la configuración completa de las políticas de seguridad de la plataforma.
    - Quedarán excluidas aquellas soluciones que requieran una plataforma de gestión externa para gestionar y administrar la solución.
    - Creación de diferentes tipos de usuario para la administración, pudiendo aplicar distintos roles o perfiles, así como definir redes de origen confiables. También es necesario disponer de la posibilidad de crear usuarios de tipo REST-API.
    - Todos los cambios efectuados en los cortafuegos deben aplicarse de forma inmediata, sin necesidad de compilar o realizar acciones similares.
    - Soporte de SNMP y sFlow.
    - Exportación de logs vía SYSLOG, FTP, SCP y TFTP.
- *Networking*
    - Soporte de los protocolos RIP v1/v2, OSPF, ISIS, BGP, WCCP y Multicast para IPv4 e IPv6, enrutamiento basado en políticas (PBR) y funcionalidades avanzadas de SD-WAN.
    - Soporte de VRFs (múltiples tablas de enrutamiento) y enrutamiento multiVRF (para BGP y OSPF).
    - Soporte Dual Stack IPv4 e IPv6 simultáneamente.
    - Network Address Translation NAT IPv4, NAT64 i NAT66.
    - DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.
    - 802.1Q VLANs y Point-to-Point Protocol over Ethernet (PPPoE).
    - 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.
    - Capacidad de balanceo de servidores a nivel 4 para todos los servicios, así como posibilidad de realizar *SSL off-loading* para el tráfico HTTPS.
    - La solución de seguridad debe contar con capacidades integradas de SD-WAN, en concreto:
        - Balanceo inteligente de conexiones físicas y lógicas, independientemente del tipo de conexión WAN (MPLS, 3G/4G, FTTH, VPN, etc.).
        - El número mínimo de conexiones físicas y lógicas que se pueden añadir a la SD-WAN debe ser de 256.
        - Verificación de la disponibilidad de Internet para cada una de las líneas, mediante los protocolos http, ping, dns y TWANP. El número mínimo de *health-checks* debe ser de 100.
        - Verificación de calidad en tiempo real: *jitter*, pérdida de paquetes (*packet loss*) y latencia por línea.

- Configuración de políticas de SD-WAN inteligente basadas en el origen (usuarios de Active Directory y dirección IP), en el destino (dirección IP, aplicaciones y/o servicios de Internet/aplicaciones) y en la línea con mejor calidad en ese momento, basada en valores de jitter, pérdida de paquetes, latencia, tráfico de subida/bajada o ancho de banda, así como una combinación ponderada por pesos.
- En caso de que se requiera licenciamiento o suscripciones para activar estas funcionalidades, será necesario que estén incluidas en la propuesta durante toda la duración del contrato.

o Soporte de VXLAN y VXLAN VTEP para la extensión de nivel 2 sobre redes de nivel 3.
o El sistema propuesto debe contar con una funcionalidad integrada de Traffic Shaping tanto para el tráfico saliente como entrante, siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este Traffic Shaping debe estar basado en aplicaciones y URL globales por perfil o por dirección IP.

Las funcionalidades y los requisitos mínimos solicitados para los dos equipos MFA son los siguientes:

- Los dos equipos MFA deben ser en formato *appliance* de un único fabricante (el mismo que los cortafuegos), quedando excluidos los servidores de propósito general y las máquinas virtuales. Deben poder instalarse en un bastidor estándar de 19".
- Los dos equipos físicos deben tener características idénticas, estar redundados y en alta disponibilidad (HA, *High Availability*). Deben permitir trabajar en modo HA activo-activo y activo-pasivo. En caso de activar sistemas virtuales, estos pueden funcionar en cualquiera de los dos nodos, de forma que se consiga un activo-activo.
  - La transferencia de servicio de un equipo al otro debe poder realizarse sin cortes, sin pérdida de conexiones TCP ni interrupción del servicio.
  - Las configuraciones deben transferirse automáticamente entre los dos equipos.
  - En caso de que se requiera licenciamiento o suscripciones para activar la alta disponibilidad, será necesario que estén incluidas en la propuesta durante toda la duración del contrato.
- Autenticación centralizada de usuarios y máquinas.
- Integración con autenticación de doble factor.
- Integración con autenticación de doble factor como servicio.
- Arquitecturas de *Single Sign-On*.
- Gestión de invitados.
- Capacidades requeridas para la plataforma de gestión de identidades para los servicios de autenticación
  - Debe poder ejercer tanto el rol de servidor de autenticación como el de cliente de otros repositorios o fuentes de identidad.
  - Debe poder operar como un servidor autónomo de RADIUS y TACACS+, ofreciendo autenticación tanto basada en certificados como no basada en ellos, como EAP-TLS, EAP-TTLS, PEAP, EAP-GTC, y también autenticación MAC

para entornos con MAB (*Mac Authentication Bypass*). Debe permitir proteger las conexiones RADIUS mediante el uso de RADSec (RADIUS sobre TLS).
    - Debe poder conectarse a un servicio LDAP (Microsoft Active Directory, OpenLDAP/Gsuite) para solicitar la validación de usuarios, por ejemplo, cuando recibe una petición RADIUS.
    - Debe poder integrarse con el Active Directory de Windows, al menos para permitir verificar que una máquina que intenta acceder a la red haya sido registrada y contenga credenciales válidas, realizando una autenticación de máquina previa a la autenticación basada en usuario.
    - Debe permitir desplegar portales de autenticación explícita para una autenticación manual, por ejemplo, en casos de uso como la gestión de invitados (donde el usuario ni siquiera pertenece a la organización).
    - Debe ser compatible con OAUTH para integrar la autenticación con redes sociales (al menos Facebook, Google, LinkedIn, Twitter), Azure Directory y G-Suite.
- Capacidades requeridas para la plataforma de gestión de identidades para el *Single Sign-On* (SSO):
    - Debe disponer de la capacidad de integrarse con otros servicios de autenticación disponibles en la red interna, con el fin de asegurar que cada usuario solo tenga que autenticarse una vez, y que dicha autenticación se reutilice en el resto de sistemas.
    - Debe poder detectar qué usuarios han iniciado sesión en el Directorio Activo, así como permitir integraciones vía syslog, NTLM y SAML (tanto en el rol de *Service Provider* [SP] como de *Identity Provider* [IdP]).
- Capacidades requeridas para la plataforma de gestión de identidades para el doble factor de autenticación:
    - Debe proporcionar una solución de doble factor de autenticación segura que garantice que solo los usuarios autorizados tengan acceso a la información crítica, aportando una capa adicional de seguridad que reduce drásticamente la posibilidad de pérdida de información.
    - El uso de este segundo factor será muy amplio, abarcando tanto la autenticación de accesos remotos vía VPN, como la autenticación en aplicaciones y portales, pudiendo incorporarse también a la administración de sistemas y plataformas de seguridad y servicios corporativos críticos.
    - La plataforma solicitada debe soportar diferentes tipos de *tokens* concurrentes, tanto físicos como virtuales, además de doble factor basado en correo electrónico o SMS.
    - Para facilitar la gestión de usuarios, debe incluir portales de autorregistro, aprovisionamiento automático de *tokens* y recuperación de contraseña.
- Capacidades requeridas para la plataforma de gestión de identidades para los *tokens*:
    - Se requiere la provisión de una solución de OTP (*One Time Password*) o *token* para 500 usuarios.
    - Debe proporcionarse en formato de aplicación móvil (compatible con los sistemas Android, iOS y Windows Mobile), y debe contemplarse la posibilidad

futura de disponer de *tokens* físicos (en formato tarjeta de crédito/visita o llave USB) para algunos casos particulares.
    - Debe soportar notificaciones *push*, es decir, que el usuario solo tenga que pulsar para aceptar la autenticación y que el *token* sea enviado automáticamente a la plataforma de gestión de identidades, simplificando la interacción entre el sistema de autenticación y el usuario, sin necesidad de que este introduzca los dígitos uno a uno.
    - Esta solución no debe requerir soporte recurrente, por lo que la licencia debe ser perpetua.
- Disponer del siguiente número mínimo de puertos:
    - 1 puerto de consola.
    - 1 puerto USB para permitir la instalación desatendida del firmware y la aplicación de configuración durante el arranque del equipo, con el fin de realizar tareas automáticas de instalación y mantenimiento.
- Cada uno de los equipos del sistema MFA debe disponer de:
    - 4 x GE RJ45
    - Disco duro de hasta 1 TB en formato HDD
    - Consumo eléctrico inferior a 270 W con todos los puertos ocupados
    - Fuente de alimentación doble
- Capacidad de gestión de los equipos mediante acceso vía web (https), prescindiendo de interfaces basadas en Java, y terminal (ssh) para la configuración completa de las políticas de seguridad de la plataforma.
    - Quedarán excluidas aquellas soluciones que requieran una plataforma de gestión externa para gestionar y administrar la solución.
    - Creación de diferentes tipos de usuario para la administración, pudiendo aplicar distintos roles o perfiles, así como definir redes de origen confiables. También es necesario disponer de la posibilidad de crear usuarios de tipo REST-API.
    - Todos los cambios efectuados en los cortafuegos deben aplicarse de forma inmediata, sin necesidad de compilar o realizar acciones similares.
    - Soporte de SNMP y sFlow.
    - Exportación de logs vía SYSLOG, FTP, SCP y TFTP.

La oferta deberá incluir todos los elementos de red necesarios para poder integrar el sistema en el equipamiento de red con arquitectura *spine-leaf*, que se detalla en la Figura 1 como FW Perimetrales, garantizando su compatibilidad y redundancia (conectores SFP necesarios en ambos extremos y cableado).

Adicionalmente, la solución podrá proveer un sistema de *logging* y *reporting* (instalado en una máquina virtual/appliance) para que los cortafuegos envíen en tiempo real los logs generados, con las siguientes funcionalidades:

- Monitorización en tiempo real del tráfico filtrado por los distintos módulos de los equipos.

- Monitorización histórica externa a los dispositivos, almacenamiento de *logs*, informes del tráfico analizado por los equipos con capacidad para generar reportes de aproximadamente 6 meses.
- Informes y alertas en función de direcciones, puertos, protocolos.
- Análisis, correlación e informes de la información de seguridad de forma centralizada.
- Panel de control con vista general de usuarios destacados, aplicaciones, destinos, sitios web, vulnerabilidades, etc.
- Gestión de eventos con generación de alertas automáticas.
- Visor de *logs* en tiempo real o histórico, que permita la visualización de tráfico, eventos y seguridad.
- Capacidad de filtrado y granularidad en el análisis de *logs*.
- Posibilidad de generación de alertas por niveles de seguridad, eventos específicos, acciones o destinos y número de eventos en un tiempo determinado.
- Notificación de alertas por correo electrónico, SNMP o syslog.
- Rotación automática de los *logs* recopilados con envío de históricos a otros sistemas por email, FTP, HTTP, etc.
- Vista comparativa de patrones de tráfico y amenazas.
- Análisis exhaustivo de todas las actividades relacionadas con el tráfico y los dispositivos.
- Elaboración de informes sobre todas las actividades de tráfico y de dispositivos.

Dado que la organización dispone actualmente de equipamiento de seguridad de la marca Fortinet, y que este se ha integrado con el actual sistema de Web Application Firewall (WAF), el cual no está previsto que se modifique, se requiere que cualquier solución propuesta sea plenamente compatible e integrable con el equipamiento Fortinet existente.

Con el objetivo de garantizar la continuidad operativa, la eficiencia en la gestión centralizada de la seguridad y la coherencia con la arquitectura de seguridad implementada, se valorará positivamente que la solución propuesta pertenezca al mismo fabricante (Fortinet) o que ofrezca total garantía de integración nativa con los sistemas actuales.

3.2. Requisitos específicos del equipamiento del lote 2

El objetivo de este lote es la renovación del equipamiento de la red del Centro de Procesamiento de Datos, la red de gestión fuera de banda y la red interna.

La red actual está compuesta por diferentes segmentos de comunicación, incluyendo redes públicas, privadas y de gestión, cada una con funcionalidades específicas dentro del centro de procesamiento de datos y la infraestructura de red de acceso y servicios internos. Estas redes están actualmente configuradas sobre un equipo principal de núcleo Cisco Nexus 9500, equipado con doble supervisora, que actúa principalmente como conmutador de nivel 2. No obstante, también asume funcionalidades de nivel 3, como el peering BGP con el equipamiento troncal de la Anella Científica (a través de los cortafuegos en modo transparente) y la gestión del direccionamiento IP público de los usuarios, que disponen de direcciones IP públicas fijas.

En los conmutadores Cisco N5K se asumen principalmente funciones de distribución y acceso en capa 2 dentro del centro de datos. Adicionalmente, gestionan el nivel 3 para el direccionamiento privado de los servicios. Junto con estos equipos, también se dispone de conmutadores Huawei CE16800, hacia los cuales se está migrando progresivamente la funcionalidad de nivel 3 de los servicios privados. Tanto los N5K como los CE16800 están desplegados en configuración redundante, garantizando la continuidad del servicio y la alta disponibilidad de la infraestructura de red.

Además, se dispone de una red adicional compuesta por conmutadores de acceso de diversos fabricantes (Cisco, HP, etc.), que no cuentan con redundancia en sus elementos de hardware. Esta red tiene como función principal la gestión y monitorización, aunque, en casos puntuales, algunos de estos dispositivos también son utilizados para transportar VLANs de servicio. Esta situación se da principalmente en entornos donde, por limitaciones de cableado o cobertura en el momento de la instalación, no fue posible implementar una alternativa específica.

La red de gestión fuera de banda es una red paralela e independiente del resto de la infraestructura, dedicada casi en exclusiva a tareas de administración y monitorización de los equipos de red, servidores y sistemas del centro de procesamiento de datos. Esta red está diseñada para ofrecer un acceso estable, seguro y aislado, incluso en situaciones de fallo de la red principal, y dispone de un mecanismo de acceso remoto de contingencia para permitir la gestión de los equipos en caso de incidencias graves o desconexión de la red de producción.

Finalmente, la red interna proporciona conectividad a servicios de la organización, y es utilizada por usuarios, sistemas y aplicaciones corporativas. Esta red soporta tanto tráfico de usuario como flujos de datos entre servicios internos, y puede incluir segmentos diferenciados según áreas funcionales (como recursos humanos, gestión económica, etc.). Se encuentra integrada dentro de la topología general del centro de datos, pero mantiene una segmentación lógica y política de seguridad propia, con el objetivo de garantizar la confidencialidad y la disponibilidad de los servicios corporativos.

La renovación de la red incluirá una actualización de esta con el suministro de una solución de equipamiento de conmutación y encaminamiento para el núcleo de red del centro de datos en arquitectura *spine-leaf* basada en Fabric VXLAN con enlaces de 100 G.

Con esta arquitectura se busca disponer de una mayor redundancia, una mayor anchura de banda, mejorar la escalabilidad y reducir la latencia.

La capa spine estará formada por los conmutadores que realizarán el encaminamiento y funcionarán como el núcleo de la red.

Las funcionalidades y los requisitos mínimos solicitados para los *spine* son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19”.
- Debe estar compuesto por dos equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:

- 8 x 100 GE QSFP28
- 8 transceptores QSFP28-100G-SR4
- Consumo eléctrico máximo de 1600 W con todos los puertos ocupados
- Fuente de alimentación doble

La capa *leaf* incluye tres niveles:

- *Server leaf*, donde se conectan los servidores, dispositivos de almacenamiento y equipos de cálculo científico.
- *Service leaf*, donde se conectan los cortafuegos perimetrales y los cortafuegos del centro de procesamiento de datos.
- *Border leaf*, donde se conecta la Anella Científica y los conmutadores de los usuarios finales.

Las funcionalidades y los requisitos mínimos solicitados para el *service leaf* son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por dos equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
  - 4 x 100 GE QSFP28
  - 4 transceptores QSFP28-100G-SR4
  - 2 x 25 GE SFP+
  - 4 transceptores SFP28-25G-SR
  - 8 x 10 GE SFP+
  - 16 transceptores SFP+
  - Consumo eléctrico máximo de 1300 W con todos los puertos ocupados
  - Fuente de alimentación doble

Las funcionalidades y los requisitos mínimos solicitados para el *border leaf* son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por dos equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
  - 6 x 100 GE QSFP28
  - 5 transceptores QSFP28-100G-SR4
  - 1 transceptor Cisco 100G SR4
  - 4 x 25 GE SFP+
  - 8 transceptores SFP28-25G-SR
  - 2 x 10 GE SFP+
  - 4 transceptores SFP+
  - Consumo eléctrico máximo de 1300 W con todos los puertos ocupados
  - Fuente de alimentación doble

El *server leaf* estará compuesto por dos conmutadores Huawei CE16804 ya instalados en el centro de procesamiento de datos.

Adicionalmente, se deben proporcionar tres conmutadores para disponer de conexiones de cobre 10G (actualmente en el equipamiento Cisco Nexus 9500) en la nueva infraestructura *leaf-spine*, con las siguientes funcionalidades y requisitos mínimos:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por dos equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
    - 2 x 25 GE SFP+
    - 4 transceptores SFP28-25G-SR
    - 48 x 10 GE RJ45
    - Fuente de alimentación doble

Con el objetivo de disponer de una gestión centralizada de la seguridad en el marco de la nueva arquitectura spine-leaf basada en tecnología Fabric VXLAN, dicha gestión se llevará a cabo mediante dos cortafuegos principales. Asimismo, se prevé la posibilidad de delegar la aplicación de políticas de seguridad a los distintos conmutadores (*spine, service leaf, border leaf* y *server leaf*) que integran la infraestructura.

Las funcionalidades y los requisitos mínimos solicitados para los cortafuegos del centro de procesamiento de datos (*FW-Datacenter en la Figura 1*) son los siguientes:

- Los cortafuegos deben poder instalarse en un bastidor estándar de 19".
- Los equipos cortafuegos deben ser en formato *appliance* de un único fabricante, quedando excluidas las máquinas virtuales y los servidores de propósito general. Deben poder instalarse en un bastidor estándar de 19".
    - Los dos equipos físicos deben ser de características idénticas, redundantes y en alta disponibilidad (*HA, High Availability*). Deben permitir trabajar en modo *HA activo-activo* y *activo-pasivo*. En caso de activar sistemas virtuales, estos pueden funcionar en cualquiera de los dos nodos, de forma que se consiga un activo-activo.
    - La transferencia de servicio de un equipo al otro debe poder realizarse sin cortes, sin pérdida de conexiones TCP ni interrupción del servicio.
    - Las configuraciones deben sincronizarse automáticamente entre los dos equipos.
    - En caso de requerir licencias o suscripciones para activar la alta disponibilidad, estas deberán estar incluidas en la propuesta durante toda la duración del contrato.
- IPv4 Firewall Throughput (1518/512/64-byte, UDP) de 240/240/120 Gbit/s
- IPv6 Firewall Throughput (1518/512/64-byte, UDP) de 240/240/75 Gbit/s
- Cada uno de los equipos cortafuegos debe disponer de:
    - 2 x 25 GE ZSFP+
    - 2 transceptores SFP-25G-SR

- Consumo eléctrico máximo de 900 W con todos los puertos ocupados
- Fuente de alimentación doble

Las funcionalidades y los requisitos mínimos solicitados para el concentrador de los equipos de gestión fuera de banda (*MNGT en la Figura 1*) son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por un único equipo físico.
- Cada uno de los equipos conmutadores debe disponer de:
  - 2 x 25 GE SFP+
  - 4 transceptores SFP28-25G-SR
  - 24 x 10 GE SFP+
  - 10 transceptores SFP+

Las funcionalidades y los requisitos mínimos solicitados para los equipos de gestión fuera de banda que estarán conectados al concentrador (*MNGT en la Figura 1*) son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por cinco equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
  - 4 x 10 GE SFP+
  - 4 transceptores SFP+
  - 48 x 10 GE RJ45 10/100/1000

Las funcionalidades y los requisitos mínimos solicitados para los equipos de la red interna del *CPD* y de la *Seu 1* son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por cuatro equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
  - 4 x 10 GE SFP+
  - 4 transceptores SFP+
  - 24 x 10 GE RJ45 10/100/1000

Las funcionalidades y los requisitos mínimos solicitados para los equipos de la red interna de la *Seu 1 - Planta* y de la *Seu 2* son los siguientes:

- Los conmutadores deben poder instalarse en un bastidor estándar de 19".
- Debe estar compuesto por cuatro equipos físicos, que deben ser de características idénticas.
- Cada uno de los equipos conmutadores debe disponer de:
  - 4 x 10 GE SFP+

- 2 transceptores SFP+
- 48 x 10 GE RJ45 10/100/1000

También se requerirá el suministro de cables de red RJ45 de Categoría 6 o superior, con conectores ya montados y protegidos, y con las siguientes longitudes y cantidades:

- Diez (10) unidades de 20 metros
- Veinte (20) unidades de 15 metros
- Cuarenta y cinco (45) unidades de 10 metros
- Cuarenta (40) unidades de 5 metros

Todo el equipamiento de electrónica de red solicitado en este lote se resume en la siguiente tabla.

Equipament de xarxa		
Commutadors *Spine*	2	Commutadors amb 8 ports 100G
Commutadors *Border Leaf*	2	Commutadors amb 6 ports 100G + 2 ports 10G
Commutadors *Service Leaf*	2	Commutadors amb 4 ports 100G + 2 ports 25G + 8 ports 10G
Commutadors RJ45 10G	3	Commutadors 2 ports a 25G + 24 ports a 10G RJ45
Commutadors MGMT	1	Commutador 2 ports a 25G + 24 ports a 10G
Commutadors Seu 1 - Panta, Seu 2 i TOR MGMT	9	Commutadors 2 ports a 10G + 48 ports a 10/100/1000 RJ45
Commutadors CPD i Seu 1	4	Commutadors 4 ports a 10G + 24 ports a 10/100/1000 RJ45
Firewalls gestió Datacenter	2	

La oferta deberá incluir una solución avanzada para la gestión automatizada, inteligente y centralizada de las redes del centro de procesamiento de datos, incluidas las de fuera de banda e internas, especialmente aquellas basadas en arquitecturas *spine-leaf* con VXLAN EVPN.

Esta solución deberá instalarse en servidores físicos proporcionados por el licitador, los cuales deberán incluirse como parte del equipamiento suministrado.

Los servidores deberán contar con la capacidad, redundancia y prestaciones necesarias para garantizar el alto rendimiento y la disponibilidad de la plataforma de gestión, incluyendo soporte para alta disponibilidad y actualizaciones sin interrupción del servicio.

Las funcionalidades y requisitos mínimos solicitados para la gestión automatizada de las redes del centro de procesamiento de datos son los siguientes:

- Gestión centralizada de la red del centro de datos, incluyendo electrónica de red, topologías y servicios.
- Automatización de la configuración y despliegue de la red (zero-touch provisioning, ZTP).
- Control de políticas de seguridad distribuidas entre los dispositivos (microsegmentación).
- Visibilidad en tiempo real del estado de la red y análisis de rendimiento.
- Diagnóstico inteligente y localización de fallos asistida por IA.

- Soporte para redes VXLAN EVPN, que permiten el aislamiento de servicios y la virtualización de la red.
- Integración con cortafuegos y servicios de seguridad, como por ejemplo la delegación de reglas a los conmutadores.
- Topología lógica y física unificada en un diagrama.
- Monitorización de redes SDN y redes tradicionales.
- Monitorización de la electrónica de red (CPU, RAM, etc.).
- Tráfico de entrada y salida en todas las interfaces físicas (puertos) y lógicas (agregación de enlaces), tanto en paquetes como en bits por segundo (bps).
- Recursos por Tenant: VRF y, en función de la tecnología utilizada, Bridge Domains, el estado de las TCAM de los conmutadores, etc. (o conceptos equivalentes).
- Recogida de logs y alarmas de la electrónica de red.

Adicionalmente, se valorará el soporte para funcionalidades de monitorización avanzada que incluyan:

- Telemetría en tiempo real y capacidad de análisis de datos históricos (semanas, meses).
- Uso de inteligencia artificial para la detección, localización y sugerencia de soluciones ante incidentes o problemas de red en cuestión de minutos.
- Garantía de calidad y diagnóstico de problemas a nivel de aplicación y servicios.
- Visibilidad de cambios en la red mediante snapshots manuales o programados.
- Visualización gráfica, bajo demanda, del camino físico y virtual entre endpoints (físicos o virtuales), mostrando los switches físicos, hypervisores y servidores implicados en el camino de datos entre los dos endpoints. En esta representación deberán mostrarse atributos de red (IP, MAC) y atributos de máquina virtual (como el nombre).
- Capacidad de monitorización de redes RoCE y entornos *multi-cloud*.

Todas estas funcionalidades deberán estar disponibles mediante una interfaz gráfica unificada de administración.

Dado que la organización dispone actualmente de equipamiento de conmutación de la marca Huawei, y que este debe integrarse en la nueva arquitectura *spine-leaf* basada en Fabric VXLAN, se requiere que cualquier solución propuesta sea plenamente compatible e integrable (de forma nativa) con el equipamiento Huawei existente.

Con el objetivo de garantizar la continuidad operativa, la eficiencia de la gestión centralizada de la seguridad y la coherencia con la arquitectura de seguridad implementada, se valorará positivamente que la solución propuesta pertenezca al mismo fabricante (Huawei) o que ofrezca garantías de integración nativa con los sistemas actuales.

Todos los equipos suministrados deberán ser de un único fabricante, quedando excluidas las máquinas virtuales y los servidores de propósito general.

La oferta deberá incluir todos los elementos de red necesarios para poder integrar el sistema con el equipamiento de red actual en arquitectura *spine-leaf*, red de gestión fuera de banda (*MNGT*) y red interna (*CPD*) que se detalla en la *Figura 1*, garantizando su compatibilidad y redundancia (conectores SFP necesarios en ambos extremos y cableado).

La oferta deberá incluir los servicios de instalación del equipamiento físico, configuración y migración de las redes públicas, privadas y de gestión hacia esta nueva arquitectura, incluyendo el análisis, planificación, ejecución y validación de la migración, con el mínimo impacto posible sobre los servicios existentes. Este proceso deberá contemplar la interconexión con el equipamiento existente de core y distribución, así como la reconfiguración de los segmentos de red actuales, garantizando la continuidad del servicio en todo momento. También deberán considerarse las políticas de seguridad, el direccionamiento IP existente, el tráfico entre VLANs y la integración con los sistemas de monitorización y gestión actuales.

Características necesarias de la migración:

- Integración con redes VXLAN EVPN.
- Reconfiguración de los servicios existentes sin interrupciones.
- Compatibilidad con los mecanismos de autenticación y control de acceso actuales.
- Documentación completa de la nueva arquitectura y configuraciones.

La migración se realizará en dos fases diferenciadas:

- Fase 1: Despliegue de la infraestructura SDN-DCN y conexión con la red de producción. Esta fase deberá incluir la puesta en marcha de los elementos *spine-leaf*, la configuración de la red VXLAN EVPN y el establecimiento de los mecanismos de gestión y monitorización centralizada.
- Fase 2: Migración de los conmutadores CE16804 hacia la nueva arquitectura como conmutadores de tipo *server leaf*, con la reasignación correspondiente de los servicios que gestionan y la integración dentro de la topología definida, garantizando redundancia y alta disponibilidad.

3.3. Requisitos específicos del equipamiento del lote 3

El objetivo de este lote es definir las condiciones técnicas que deben cumplir todas aquellas instalaciones necesarias para ampliar la capacidad del CPD ya existente, con el fin de disponer de una instalación preparada para la instalación de dos bastidores con nodos orientados a su uso en computación de alto rendimiento (HPC por sus siglas en inglés) y nodos orientados a su uso en aplicaciones de IA.

Este proyecto de ampliación del centro de proceso de datos requerirá la integración de diferentes especialidades de la ingeniería (eléctrica, climatización, control, etc.), que se verán reflejadas en este pliego de condiciones. Deberá contemplar la ampliación, modificación o adaptación de los siguientes sistemas:

- Capacidad eléctrica
- Capacidad de refrigeración

La renovación y ampliación podrá declararse como finalizada una vez instalados todos los equipos y materiales, realizadas las pruebas pertinentes para cada equipo/material que los declaren en correcto funcionamiento y conformes en las inspecciones reglamentarias correspondientes. Además, deberá legalizarse reglamentariamente la instalación ante el organismo territorial competente.

3.3.1. Instalación de nuevas puertas frías

Con el objetivo de dar servicio a dos nuevos bastidores de 800 mm de ancho, destinados a nodos de computación de alto rendimiento (HPC) y aplicaciones de inteligencia artificial (IA), se llevará a cabo la extensión de las tuberías de agua fría existentes, sin interrumpir en ningún momento el funcionamiento de la climatización actual de la sala.

El estado actual de la sala puede consultarse en la *Figura 2*, mientras que la ubicación prevista de los nuevos bastidores se detalla en la *Figura 3*.

La intervención requerirá la instalación de la conexión de dos puertas frías aprovechando las válvulas de corte actuales que dan servicio a la unidad interior de climatización TRF110 (con capacidad de refrigeración de 110 kW), la cual quedará anulada.

La oferta deberá incluir:

- La instalación de tuberías por debajo del suelo técnico, partiendo de las válvulas de conexión del equipo *TRF110*.
- La conexión completa a dos puertas frías modelo *Vertiv Liebert DCD*, con una capacidad de disipación de 50 kW cada una.
- Todos los elementos de climatización asociados, incluyendo válvulas, conexiones eléctricas, hidráulicas y sonda de temperatura para regular el caudal a través del *BMS Schneider WebStation*.
- La integración de todos los nuevos componentes con el sistema de gestión climática del CPD, concretamente con el *BMS Schneider WebStation* versión 5.0.3.13010 actualmente en servicio, en coordinación con la empresa INTAC CONTROL (https://intac.es) y el CSUC.
- Cuatro (4) sensores ambientales Vertiv Geist GT3HD con el correspondiente cableado y sondas de temperatura.

3.3.2. Acondicionamiento climático para el robot de cintas

Con el objetivo de garantizar el correcto funcionamiento del robot de cintas utilizado para las copias de seguridad, es imprescindible asegurar la estabilidad de las condiciones ambientales del espacio donde se ubica. Las condiciones climáticas requeridas son:

- Temperatura controlada entre 25 °C y 30 °C.
- Humedad relativa comprendida entre el 30 % y el 50 %.
- Variaciones máximas: no se pueden superar variaciones del 10 % en un intervalo de 1 hora, y siempre deben mantenerse dentro de los márgenes indicados anteriormente.

Con el objetivo de garantizar la estabilidad de la temperatura y la humedad, se construirá un espacio cerrado específico para ubicar la máquina de copias de seguridad. Este espacio estará equipado con una unidad autónoma de expansión directa (retorno del aire caliente por la parte superior e impulsión del aire frío por la parte frontal inferior), que incluirá humidificadores y resistencias. El sistema funcionará con impulsión frontal y retorno, y estará diseñado para mantener las condiciones ambientales óptimas.

El espacio cerrado dispondrá de un acceso por la parte posterior para facilitar las tareas de mantenimiento. Tanto la parte frontal como la posterior incorporarán una abertura superior que permitirá la comunicación de aire entre ambas zonas. Este sistema de ventilación interna estará diseñado para que el flujo de aire se mantenga estanco dentro del recinto, asegurando que las condiciones ambientales se regulen exclusivamente dentro del espacio confinado, sin intercambio con el exterior.

La unidad prevista deberá incorporar una batería adicional alimentada por el gas caliente procedente del compresor, para permitir la modulación y minimizar el encendido/apagado del compresor. También deberá disponer de integración con etapas de postcalentamiento mediante resistencias modulares, con el fin de mantener las condiciones de temperatura y humedad en salas con muy baja carga térmica.

Esta unidad deberá integrarse con el sistema de gestión del centro de procesamiento de datos (BMS) y con nuestra herramienta de monitorización, mediante sensores de temperatura y humedad ubicados dentro del espacio cerrado. El volumen aproximado de este espacio será de 6 m^3, y dispondrá de puerta de acceso.

El estado actual de la sala 1 donde se ubicará este espacio se describe detalladamente en la *Figura 4*, mientras que la distribución final con la nueva ubicación del robot de cintas se especifica en la *Figura 5*.

Para poder ejecutar esta nueva instalación climática, será necesario llevar a cabo previamente las siguientes actuaciones:

- El traslado del robot de cintas (actualmente bajo garantía de mantenimiento), en coordinación con la empresa IPM (https://ipm.es) y el CSUC.
- La retirada y gestión para el reciclaje de cinco (5) bastidores existentes, con el fin de dejar suficiente espacio para la instalación del robot, de la unidad de control climático y para la construcción del recinto.

3.3.3. Ampliación del sistema de alimentación ininterrumpida (SAI)

Se prevé la ampliación del sistema de alimentación ininterrumpida con el objetivo de garantizar una capacidad de carga de 700 kW, mediante una configuración de dos (2) unidades operativas + una (1) unidad en pasivo para asegurar la redundancia del sistema. Esta ampliación se realizará manteniendo los actuales cuadros de baterías.

Los SAI existentes están configurados en redundancia N+1 y corresponden al modelo Eaton 93PM200, con extracción de aire por la parte superior y compuestos por siete (7) celdas de energía de 50 kW cada una.

Para garantizar una distribución adecuada de la energía y mantener el equilibrio de carga entre las unidades, será necesario instalar un nuevo cuadro eléctrico que permita repartir los cuatro (4) armarios de baterías entre los tres SAI.

La distribución actual de la sala SAI se encuentra detallada en la *Figura 6*, mientras que la propuesta con la incorporación del nuevo SAI y del nuevo cuadro eléctrico se recoge en la *Figura 7*.

3.3.4. Elementos eléctricos y saneamiento

Además de las actuaciones principales previstas, se incluyen dentro del alcance del proyecto las siguientes tareas adicionales:

- Saneamiento de patch panels: Será necesario llevar a cabo el saneamiento de cinco (5) patch panels de cobre. Esta actuación implica la retirada completa del cableado existente que ya no está en uso o que no cumple con los estándares de calidad y organización requeridos. La ubicación de los patch panels a sanear, así como la correspondencia entre armarios de origen (A) y armarios de destino (X), se detalla en la *Figura 6*.
- Suministro e instalación de PDU: Se requiere la compra e instalación de diez (10) unidades de Power Distribution Units (PDU), *Vertiv VP8886 Monitored*.
- Sensores ambientales: Se prevé la instalación de veinte (20) sensores ambientales para el control y monitorización de temperatura, humedad y punto de rocío. Estos sensores deberán permitir un seguimiento en tiempo real de las condiciones ambientales críticas para garantizar la continuidad del servicio y la seguridad de los equipos. Se instalarán

seis (6) sensores ambientales *Vertiv Geist GT3HD* y catorce (14) sensores ambientales *Vertiv Geist GT3HD-50* con el correspondiente cableado y sondas de temperatura.

- Extensión de armarios bastidores: Para alojar adecuadamente las nuevas PDU, será necesaria la ampliación de dos (2) armarios bastidores existentes. Esta extensión deberá permitir una instalación segura y accesible de los equipos eléctricos y de comunicaciones.

4. Instalación y configuración de los equipos

La empresa adjudicataria ejecutará las tareas de configuración que resulten de las reuniones con los responsables del CSUC, concretando los términos de las mismas. Finalmente, se generará una documentación exhaustiva de las configuraciones aplicadas una vez se hayan llevado a cabo, entregándola en soporte papel y electrónico.

Los trabajos a realizar incluyen:

- Instalación física en las instalaciones del CSUC del hardware y cableado (también para la electrónica de red), así como de los correspondientes conectores. Antes de la recepción de los equipos, el adjudicatario deberá revisar que las instalaciones técnicas (instalación eléctrica, sistemas de refrigeración, etc.) sean adecuadas para el equipamiento ofertado y sugerir, en caso de que se detecten deficiencias, aquellas mejoras o modificaciones que considere necesarias para el funcionamiento óptimo del sistema. El adjudicatario deberá proporcionar todos los componentes y material necesario para la instalación y conexión, cableado, conectores, etc.
- Configuración de los nuevos sistemas. Una vez se entreguen los equipos, el adjudicatario deberá proporcionar la asistencia técnica necesaria para la instalación y puesta en marcha del sistema, para su configuración y optimización, así como para la integración de los equipos en el entorno de trabajo del Centro.

Una vez los equipos se vayan instalando en los bastidores (sin estar en funcionamiento), el adjudicatario deberá retirar todo el embalaje asociado al equipamiento instalado de las instalaciones del CSUC ese mismo día.

El adjudicatario deberá proporcionar la documentación y un plan de formación adecuado para el personal del CSUC, que incluirá como mínimo los siguientes conceptos:

- Manual de administración de los equipos, que se entregará en formato digital y servirá al personal del CSUC como guía para llevar a cabo las tareas necesarias de configuración, explotación y soporte posterior. Este manual contendrá, como mínimo, la siguiente información:

  - Descripción general del sistema y de sus componentes y arquitectura.
  - Esquemas gráficos detallados de la distribución de los distintos componentes y su interconexión.

  - Descripción de los principales parámetros utilizados para la configuración del sistema.
  - Descripción de los principales procedimientos básicos para la administración y explotación del sistema: parada y puesta en marcha de todos los componentes, incluyendo la parada eléctrica; creación de archivos para la depuración en caso de caída del sistema, etc.

- Plan de formación para los técnicos del Centro sobre el funcionamiento y configuración de los equipos, tanto del hardware como del software, que incluirá como mínimo un curso de operación en el que deberán abordarse, como mínimo, los siguientes aspectos:

  - Introducción a las características generales del sistema: arquitectura, tecnología de los distintos componentes, etc.
  - Herramientas de administración y gestión.
  - Principales procedimientos de operación.
  - Monitorización del sistema y optimización.
  - Seguridad de los equipos.

- Se requerirá que el licitador ofrezca formación para un máximo de 10 técnicos del CSUC interesados en:

  - Lote 1: sistema de cortafuegos redundado para el centro de procesamiento de datos (2 jornadas).
  - Lote 2: solución del equipamiento de conmutación y encaminamiento para el núcleo de red del centro de datos en arquitectura spine-leaf (3 jornadas) y solución avanzada para la gestión automatizada, inteligente y centralizada de las redes del centro de procesamiento de datos (3 jornadas).

5. Garantía de soporte

Los equipos ofrecidos deberán incluir un período mínimo de **garantía de soporte de cinco años** para todo el hardware y software suministrado.

El nivel de servicio no podrá ser inferior al siguiente:

  - **Incidencia de prioridad alta**: cuando, debido a la misma, se produzca una afectación total o una reducción del rendimiento estándar en un 15 % de los servicios ofrecidos por el CSUC. El tiempo de respuesta desde su inicio deberá ser como máximo de 2 horas naturales y el tiempo de resolución como máximo de 8 horas naturales.
  - **Incidencia de prioridad media**: cuando los *logs* o mensajes de error de los equipos indiquen que se ha producido una alteración no esperada en su comportamiento, o bien cuando se haya producido algún error que deba corregirse. El tiempo de

respuesta desde su inicio deberá ser como máximo de 8 horas naturales y el tiempo de resolución como máximo de 24 horas naturales.

- **Incidencia de prioridad baja**: cuando sea de carácter informativo. El tiempo de respuesta desde su inicio deberá ser como máximo el siguiente día laborable y el tiempo de resolución como máximo de 5 días laborables.

En caso de producirse una incidencia de prioridad alta, el CSUC podrá solicitar al adjudicatario informes puntuales sobre incidencias concretas, los cuales deberán estar disponibles en un plazo máximo de 3 días laborables.

El incumplimiento de estos plazos será penalizado según lo dispuesto en el apartado O del Cuadro de características del Pliego de Cláusulas Administrativas Particulares.

Se entiende por tiempo de atención el tiempo transcurrido desde que se notifica una incidencia hasta el inicio de las tareas necesarias para su resolución, y por tiempo de resolución el tiempo invertido en resolverla desde el momento en que se atiende hasta que queda efectivamente resuelta.

Adicionalmente, también se requiere:

- Cobertura horaria 24x7x365.
- Soporte telefónico ante incidencias y consultas con respuesta inmediata.
- Tareas preventivas: todas aquellas prestaciones necesarias para mantener los equipos solicitados en niveles óptimos de disponibilidad y funcionamiento, así como el ajuste de los elementos que permitan mantener dichos niveles. Entre otras, deberán contemplarse las operaciones de comprobación, diagnóstico y seguimiento del rendimiento de los equipos, según las especificaciones del fabricante.
- Gestión proactiva por parte del licitador de la solución propuesta para la resolución de posibles incidencias de hardware con desplazamiento al CPD.
- Revisión y actualización (si es necesario y/o por motivos de seguridad) del sistema operativo, *firmware*, mejoras de ingeniería, etc., que se realizará de acuerdo con la planificación establecida con el personal técnico del CSUC. Las revisiones del entorno y actuaciones asociadas se realizarán anualmente. Las actualizaciones por motivos de seguridad se realizarán tan pronto como esté disponible la nueva versión del sistema operativo o *firmware* que solucione el problema en la plataforma del fabricante.
- La empresa adjudicataria deberá proponer, dentro de las condiciones de garantía, tareas preventivas y correctivas del equipamiento suministrado en los términos que establece el pliego.
- Disponer de un sistema de seguimiento de incidencias y consultas mediante una base de conocimiento (preferiblemente consultable vía internet). En caso de que el licitador quiera proponer esta alternativa, deberá describir brevemente sus funcionalidades principales.

Los licitadores deberán especificar en su oferta los perfiles de los técnicos que llevarán a cabo el servicio de soporte, así como su experiencia previa en instalaciones y servicios de soporte con características similares a las del objeto del presente pliego.

En caso de incidencias críticas, el CSUC podrá solicitar al adjudicatario informes puntuales que expliquen las causas, la resolución y las medidas correctivas adoptadas. Estos informes deberán ser entregados por el proveedor al CSUC en un plazo máximo de 3 días laborables.

El licitador deberá describir en detalle los tipos de soporte disponibles y las condiciones de contratación de cada uno de ellos una vez finalizado el período de garantía, así como sus condiciones contractuales, que deberán quedar detalladas en la oferta económica del sobre C. Concretamente, deberá especificarse la política del licitador respecto a averías y reparaciones del equipamiento, la jornada laboral para incidencias y el tiempo de respuesta previsto para su resolución.

Debe tenerse en cuenta que, durante el período de garantía, todos los costes de mantenimiento deberán estar incluidos en el precio ofertado por el equipamiento.

Será necesario acreditar la posesión de la certificación del fabricante del sistema de balanceo con alta disponibilidad o de los conmutadores para la red de gestión, suficiente para ejecutar las tareas de instalación y la garantía posterior de los equipos suministrados.

La oferta deberá describir en detalle cómo se llevará a cabo la instalación y las condiciones de garantía posteriores a la instalación.

Al finalizar la instalación, el proveedor deberá entregar un inventario completo de todo el equipamiento suministrado, que deberá incluir, como mínimo, la siguiente información para cada elemento:

- Descripción del equipamiento
- Número de serie
- Part number o código del fabricante
- Importe de compra (precio unitario)

Los elementos comunes de la instalación (como el cableado, conectores, accesorios menores, etc.) podrán agruparse bajo conceptos genéricos, indicando siempre la cantidad y el coste total asociado.

Este inventario es necesario para que todo el material quede correctamente inventariado y contabilizado financieramente, y se considera un requisito imprescindible para el cierre del proyecto.

6. Prestaciones que optimizan el rendimiento de los equipos

Los licitadores podrán ofrecer prestaciones que optimicen el rendimiento de los equipos y que deberán incorporarse en el sobre que corresponda en cada caso. Estas son:

Para el lote 1:

- Incremento de la capacidad para gestionar sesiones concurrentes hasta 16 millones. (Sobre B)
- Incremento de la capacidad para gestionar nuevas sesiones por segundo. (Sobre B
- Incremento del rendimiento en nivel 7 Firewall en paquetes de 64 bytes en IPv4. (Sobre B
- Incremento del rendimiento en nivel 7 IPS. (Sobre B
- Incremento del rendimiento en nivel 7 NGFW (IPS y control de aplicaciones). (Sobre B
- Incremento del rendimiento en nivel 7 Threat Protection (IPS, control de aplicaciones y motor antimalware activos). (Sobre B
- Incremento del rendimiento para tráfico IPSEC VPN (512 bytes). (Sobre B
- Incremento del rendimiento para tráfico VPN SSL. (Sobre B
- Logging y reporting. (Sobre B)

Para el lote 2:

- Disponer de 8 puertos adicionales de 400 GE en los conmutadores *spine*. (Sobre B)
- Disponer de 12 puertos de 100 GE en los conmutadores *service leaf* y *border leaf* con sus correspondientes transceptores SR4 QSFP28. (Sobre B)
- Disponer de 24 puertos de 100 GE en los conmutadores *spine* con sus correspondientes transceptores SR4 QSFP28. (Sobre B)
- Incremento de la velocidad de los 24 puertos de los conmutadores *spine* y los 12 puertos de los conmutadores *service leaf* y *border leaf* a 200 GE con sus correspondientes transceptores SR4 QSFP56, incluidos los de la conexión a la Anilla Científica. (Sobre B)
- Disponer de 6 puertos de 100 GE en los conmutadores RJ45 y MNGT con sus correspondientes transceptores SR4 QSFP28 y 48 puertos 10GE RJ45/SFP+. (Sobre B)
- Disponer de puertos con POE en todos los conmutadores del *CPD*, *Seu 1 - Planta* y *Seu 2*. (Sobre B)
- Disponer de una solución de monitorización avanzada. (Sobre B)

Para el lote 3:

- Ampliación modular de la capacidad del SAI. (Sobre B)
- Doble puerta en el cerramiento del robot de cintas. (Sobre B)
- Ampliación del número de PDUs *Vertiv VP8886*. (Sobre B)
- Ampliación del número de sensores ambientales *Vertiv Geist*. (Sobre B)

- Jornadas extra para saneamiento de la instalación eléctrica o instalación de cableado entre bastidores. (Sobre B)

7. Duración del proyecto y plazos de entrega

Los licitadores presentarán una propuesta de cronograma, para cada lote, que distinguirá claramente cada una de las fases previstas para la ejecución del proyecto en lo que respecta a la entrega y puesta en marcha de todo el hardware y software, e incluirá como mínimo los siguientes hitos:

- Revisión de las instalaciones técnicas
- Entrega de los equipos
- Instalación y configuración del sistema
- Plan de aceptación y pruebas del equipamiento
- Plan de formación, si procede

El equipamiento deberá estar instalado y en producción como máximo el 30 de junio de 2026.

Anexo I

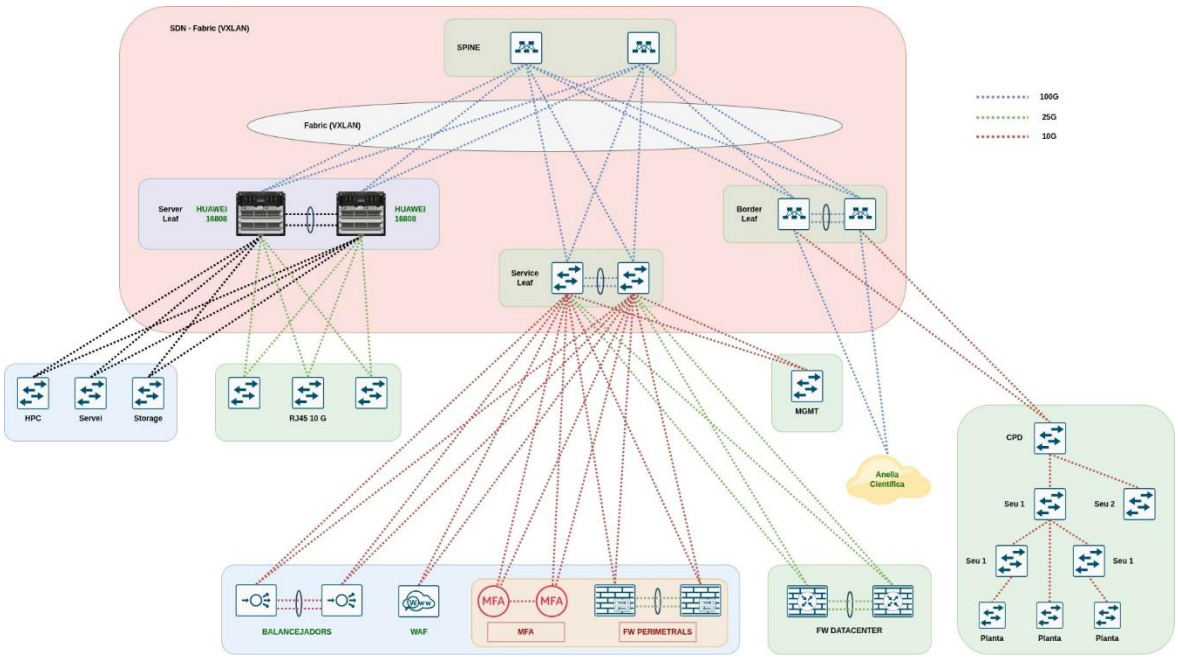

Figura 1. Esquema final del equipamiento de conmutación y encaminamiento para el núcleo de red del centro de procesamiento de datos en arquitectura *spine-leaf*.

Anexo II

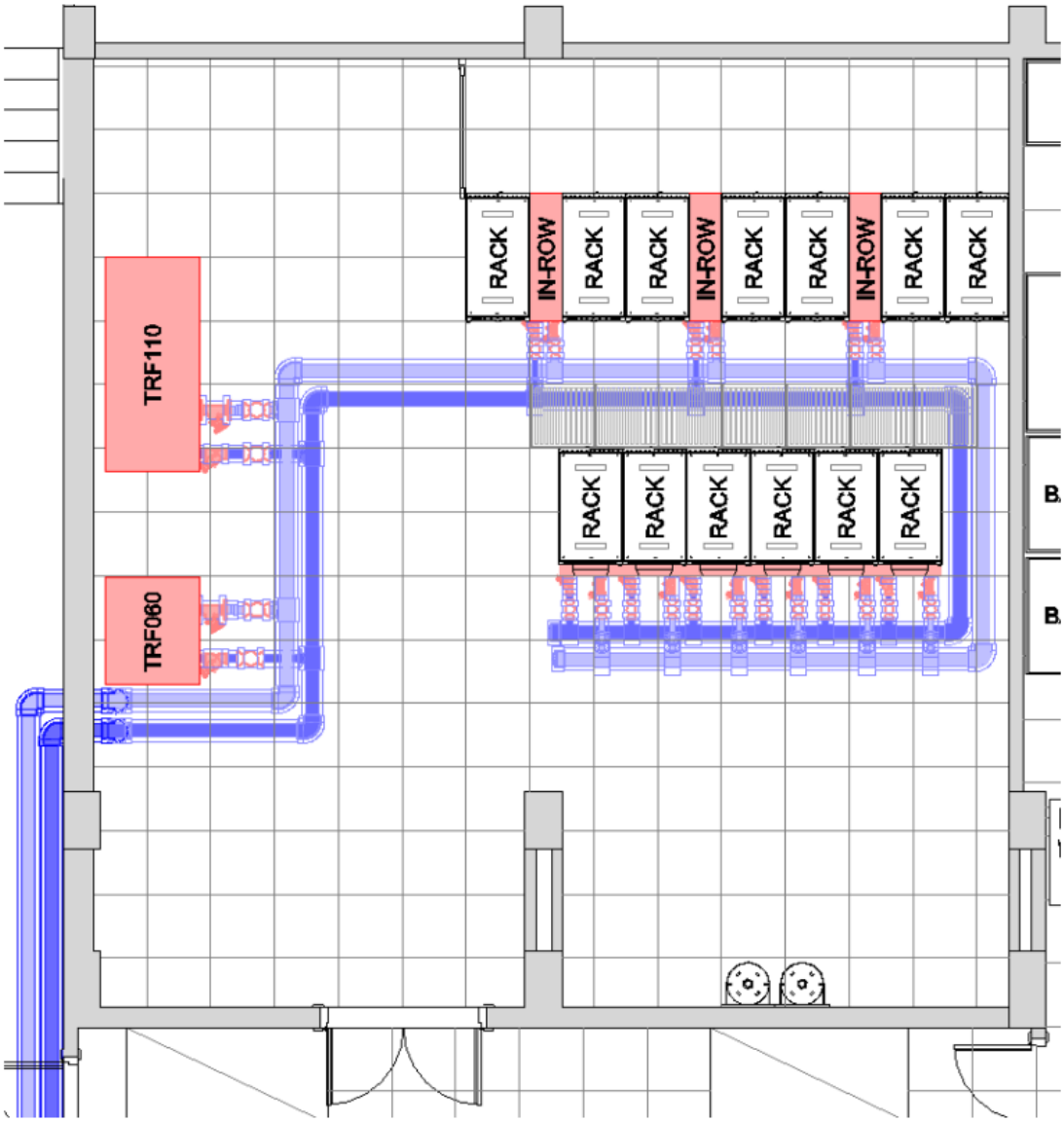

Figura 2. Estado actual de la sala 2 del centro de procesamiento de datos.

Anexo III

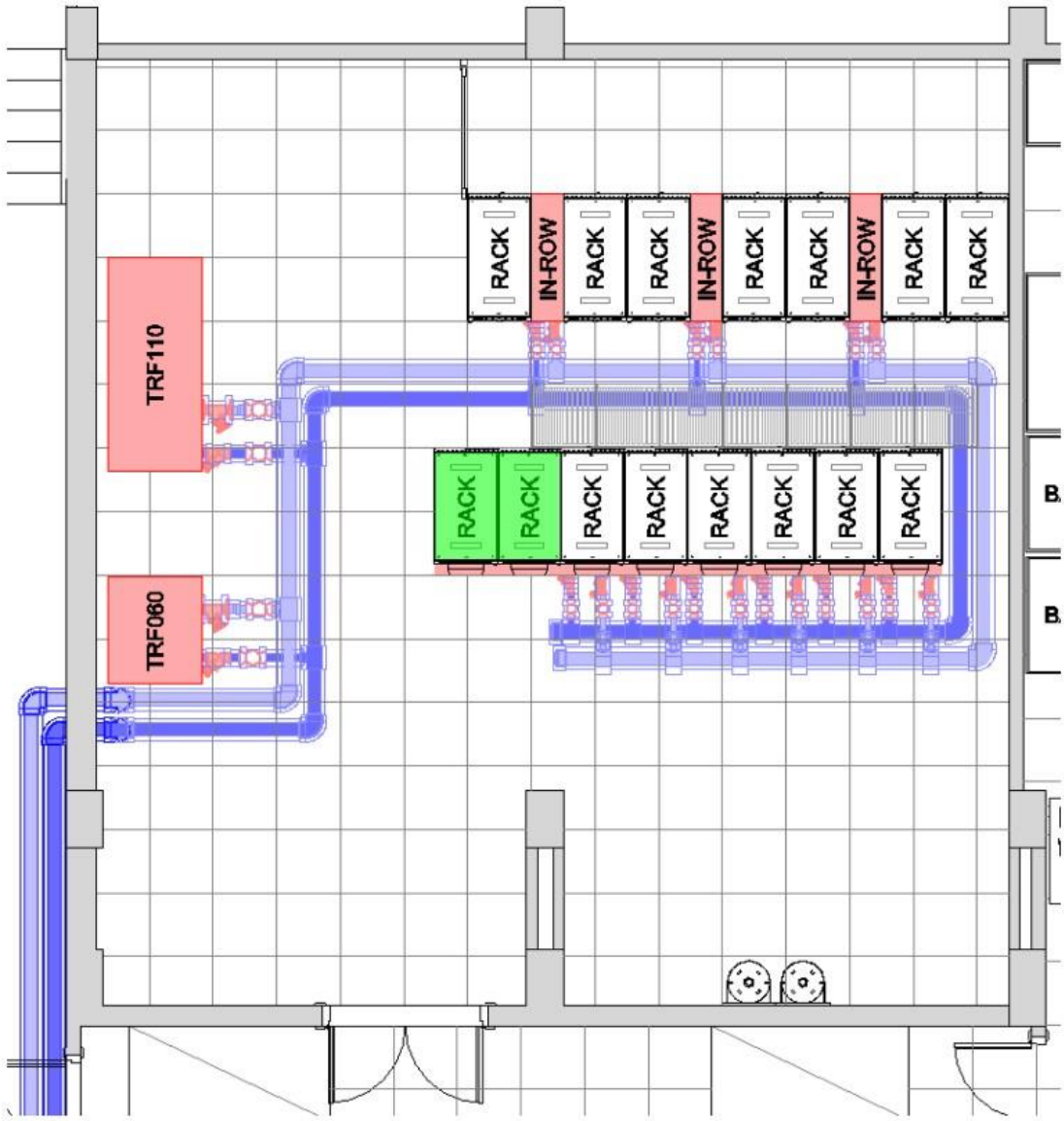

Figura 3. Propuesta de las nuevas tuberías de la sala 2 para refrigerar 2 bastidores más.

Anexo IV

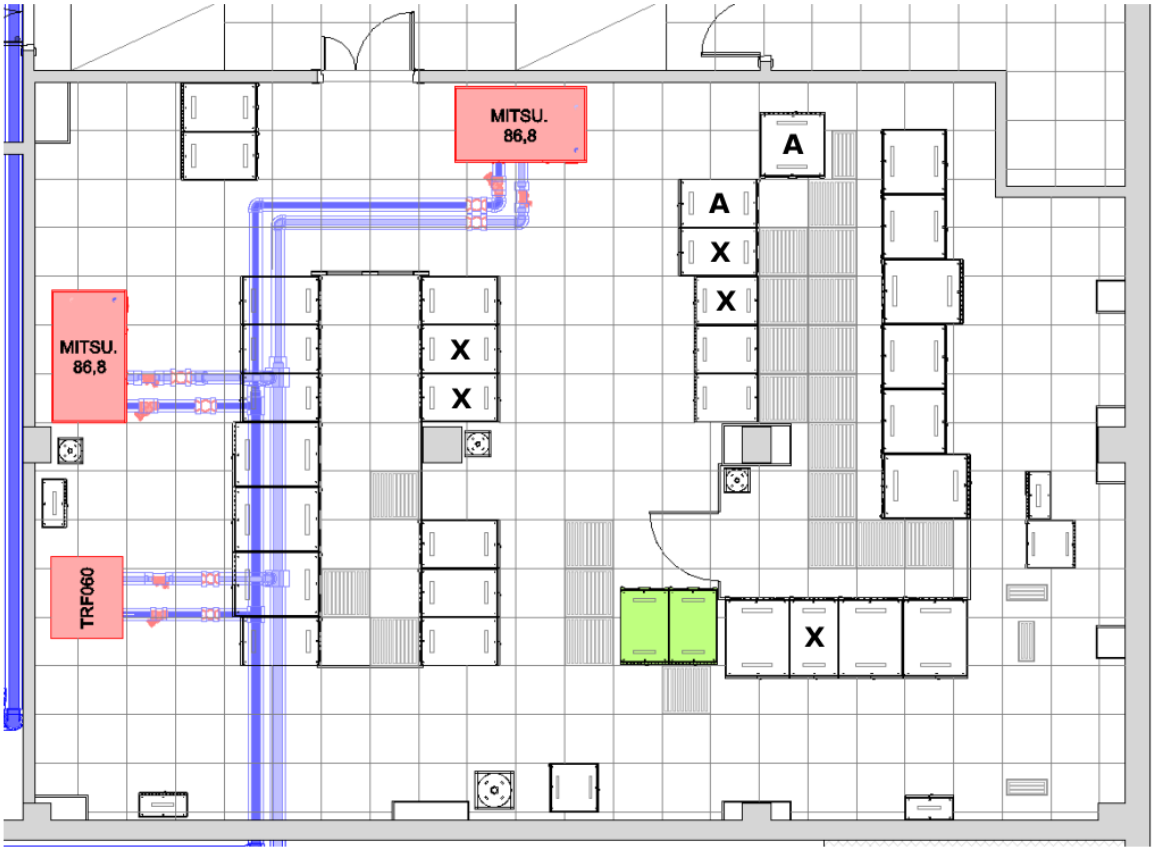

Figura 4. Estado actual de la sala 1 del centro de procesamiento de datos.

Anexo V

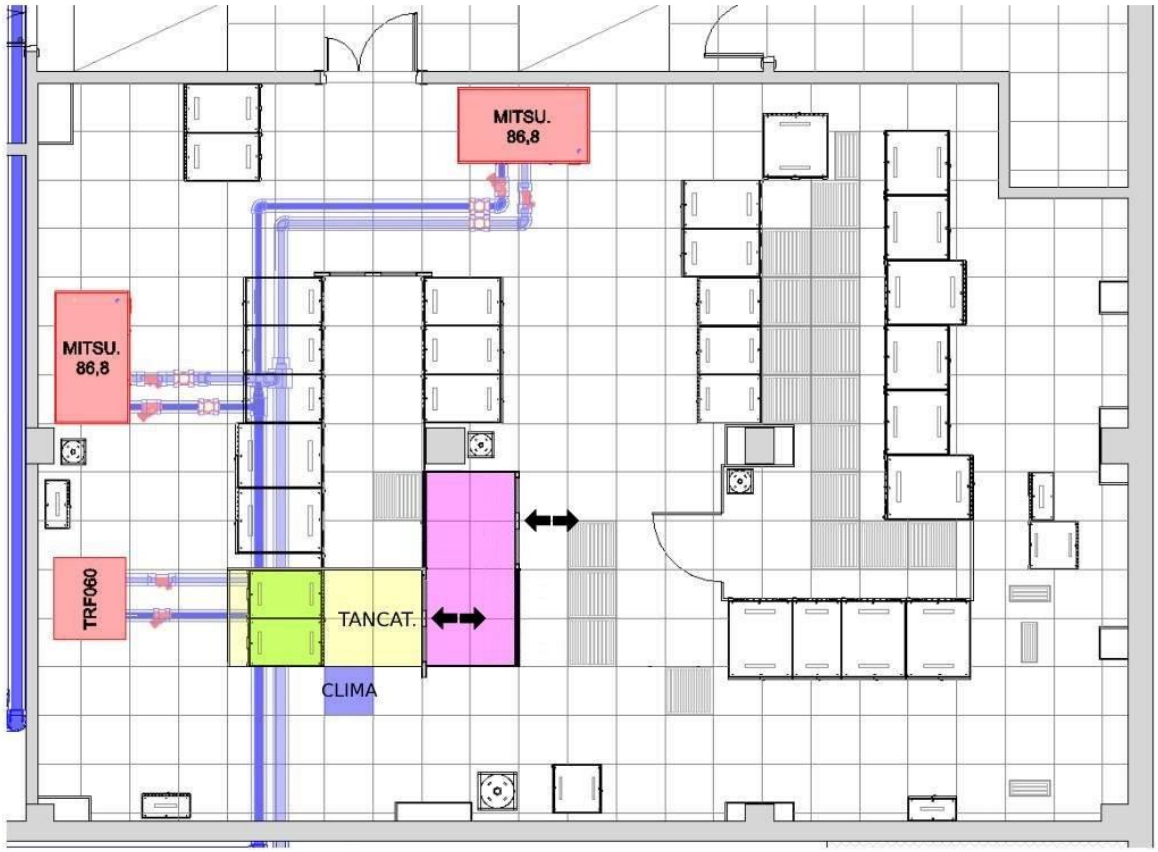

Figura 5. Propuesta de la distribución final en la sala 1 con la nueva ubicación del robot de cintas.

Anexo VI

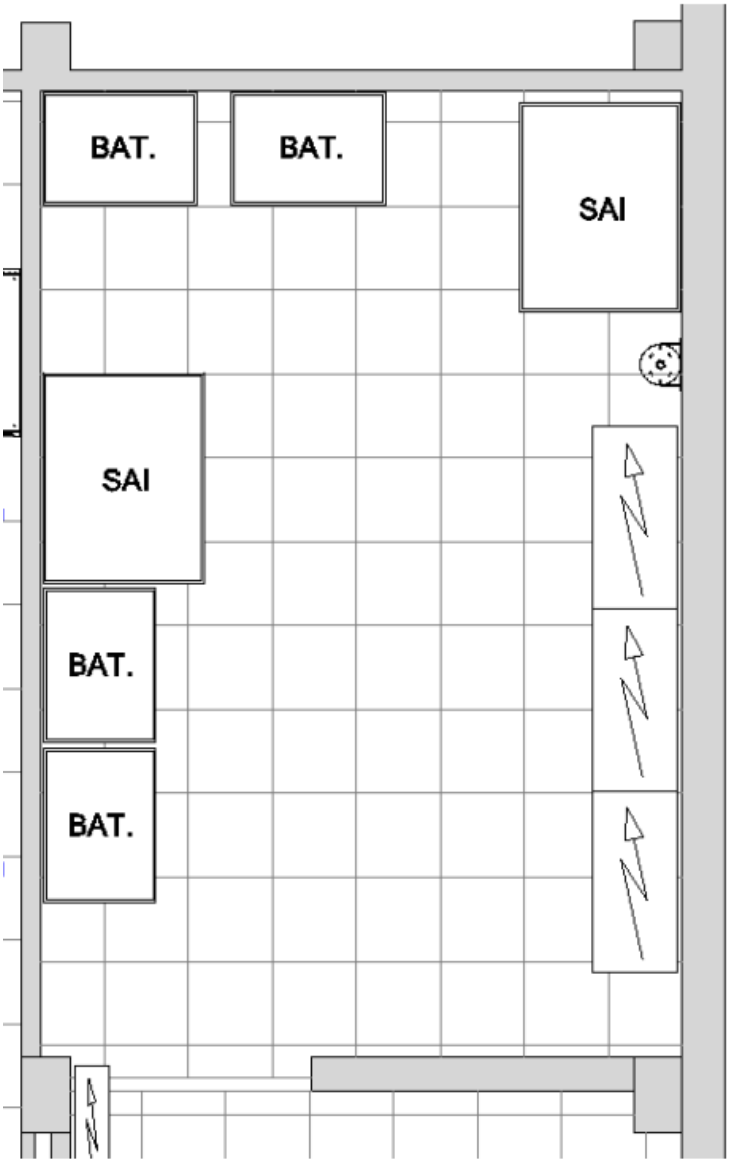

Figura 6. Distribución actual de la sala SAI.

Anexo VII

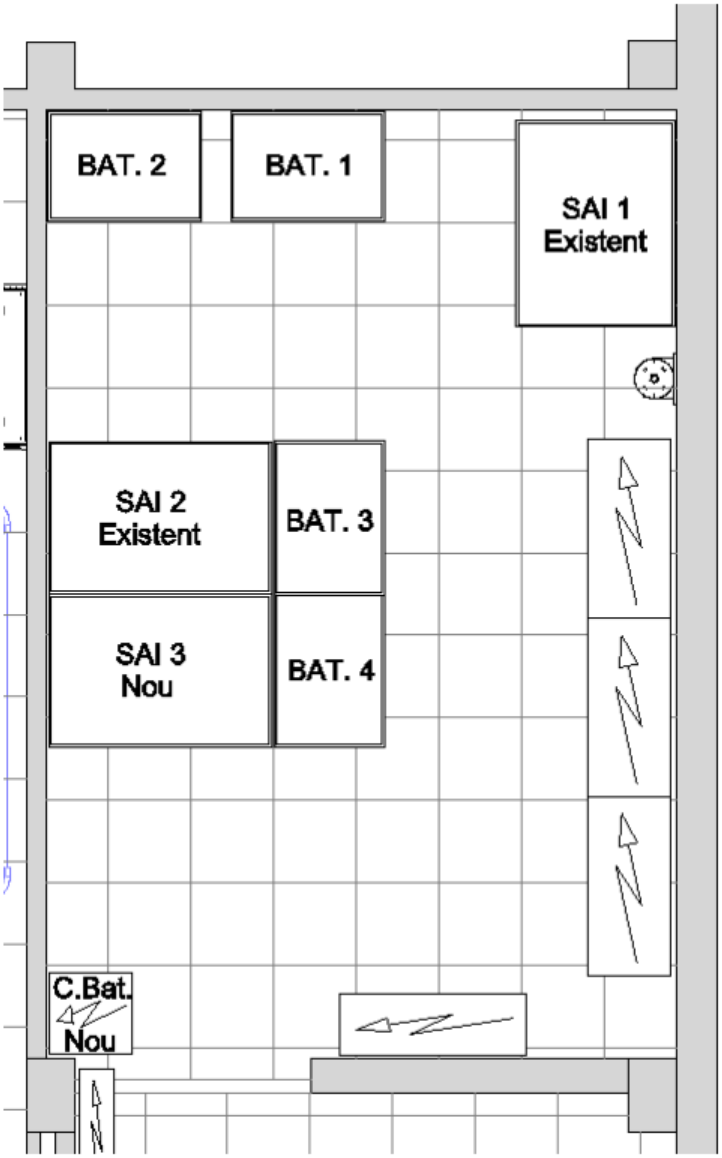

Figura 7. Propuesta de la distribución final en la sala SAI con el nuevo SAI y cuadro eléctrico.