PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA AMPLIACIÓN DEL SISTEMA DE VIRTUALIZACIÓN DEL OBSERVATORIO DE CALAR ALTO DEL CENTRO ASTRONÓMICO HISPANO EN ANDALUCÍA, A.I.E. (CAHA)

LIC-2025-005

Financiado por la Unión Europea
NextGenerationEU

MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

Índice

Financiado por la Unión Europea
NextGenerationEU
MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

1 Introducción

El Centro Astronómico Hispano en Andalucía, A.I.E. (en adelante CAHA) del Observatorio de Calar Alto cuenta desde hace siete años con un sistema de virtualización que permite albergar, dentro de una granja de cuatro ordenadores y cinco cabinas de almacenamiento (con una capacidad neta de hasta 135 TB), una gran cantidad de servidores y máquinas virtuales. Este sistema, totalmente redundante, no solo permite una gestión muy eficaz de los servidores y máquinas virtuales allí alojados, sino que también aporta un rendimiento excepcional de dichos servidores y máquinas virtuales, a la vez que ofrece varias capas adicionales de seguridad a los mismos. Además, el hecho de que en los actuales cuatro ordenadores puedan correr más de un centenar de máquinas virtuales, implica un ahorro en costes de electricidad y, por tanto, una disminución muy importante de la huella ecológica.

Desde que el sistema se puso en funcionamiento en 2018, su rendimiento ha sido espectacular y cada vez más y más servicios y aplicaciones se han ido migrando a máquinas virtuales alojadas en este sistema. Igualmente, las necesidades del observatorio se han visto incrementadas sustancialmente durante estos años, por lo que el uso que se le ha dado a la virtualización ha crecido exponencialmente, más allá incluso de las previsiones iniciales.

El presente documento define el alcance de la contratación del suministro de los elementos asociados a las Tecnologías de la Información en el Observatorio de Calar Alto (CAHA) en Almería correspondiente a la ampliación del sistema de virtualización del observatorio.

Financiado por la Unión Europea
NextGenerationEU
MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

2 Servicios y suministros objeto de este contrato

2.1 Requisitos generales

Todo el equipamiento y los componentes suministrados deben ser nuevos y, en ningún caso, usados, re-manufacturados o reacondicionados. Así mismo, tienen que estar a la venta en el momento del suministro por sus respectivos fabricantes. Este requerimiento se extiende a las garantías exigidas para dicho suministro, que necesariamente serán las proporcionadas por el fabricante.

Todos los requerimientos de los siguientes apartados tienen que considerarse como mínimos que se deben cumplir. Se aceptará equipamiento que mejore estas características.

El CAHA requerirá a los licitadores que presenten documentación oficial de los fabricantes que acrediten el cumplimiento de todos los requerimientos.

Desde el punto de vista técnico:

- Se requiere soporte nativo de todo el sistema tanto para IPv4 como para IPv6.
- Dado que en todos los casos se va a actuar sobre un sistema crítico en producción, es imprescindible minimizar el impacto sobre el sistema en funcionamiento y los usuarios del mismo. Es imprescindible, por tanto, que los equipos suministrados permitan ser integrados en la virtualización actual de una forma transparente y con el sistema en funcionamiento, sin tener que detener ningún servicio.

A efectos de que los licitadores puedan pueda ajustar sus propuestas y garanticen la plena compatibilidad oferta, el CAHA organizará una visita a las instalaciones previa a la presentación de su oferta, para informar de las instalaciones existentes a las que hace referencia el alcance de este expediente y hacer las consideraciones necesarias para el diseño y valoración de la respuesta a elaborar.

Las empresas interesadas solicitarán la asistencia a dicha visita enviando in correo concertando cita en el correo **compuhead@caha.es**. El correo deberá ser enviado en un plazo máximo de 10 días desde la fecha de publicación de este expediente.

2.2 Suministro de un servidor para virtualización

El alance de este expediente contempla el suministro de un nuevo servidor totalmente compatible con el actual sistema de virtualización, de manera que se solucione el problema de la disponibilidad de máquinas virtuales y sus servicios cuando uno de los servidores de virtualización se para por motivos de mantenimiento o por causa de fallo.

El adjudicatario deberá suministrar todo el material ofertado, siguiendo las instrucciones del CAHA y manteniendo absoluta compatibilidad con lo que ya existe. Deberá, así mismo, suministrar cualquier material necesario para su correcta instalación y funcionamiento.

2.2.1 Contexto actual y requisitos funcionales

Aunque hasta la fecha actual las capacidades de los cuatro servidores que soportan el sistema han sido válidas, empiezan a presentar problemas para gestionar adecuadamente la alta disponibilidad (HA), dado que esta requiere que, en caso de caída de uno de los servidores principales, los otros tres asuman el control inmediato de todas las máquinas virtuales que estaban funcionando en ese momento en el servidor que ha fallado.

Aunque este procedimiento es plenamente operativo en la actualidad, con la llegada de nuevos proyectos y nuevas necesidades que requerirán la adición de nuevas máquinas y servidores virtuales se incrementará el riesgo de perder esta capacidad que supone el poder levantar todas las máquinas virtuales, y sus servicios, sobre los ordenadores que no han fallado. Adicionalmente. al actualizar el firmware o software de los servidores, es necesario migrar las máquinas virtuales a otros servidores para evitar su interrupción, ya que la actualización suele requerir un reinicio. El término migrar, en este caso, hace referencia al proceso de transferir una máquina virtual de un servidor a otro sin que se requiera su detención, garantizando la continuidad del servicio y asegurando que dicha operación sea completamente transparente tanto para los usuarios como para los servicios proporcionados por la máquina virtual.

Por tanto, en el momento en que esto no sea viable, porque los recursos de los otros tres servidores principales no puedan albergar todas las máquinas virtuales del servidor a actualizar, cada vez que se actualicen los servidores de la granja, habrá que realizar paradas de algunas de las máquinas virtuales y, por tanto, de algunos de los servicios, muchos de ellos críticos, que se vienen ofreciendo desde el sistema de virtualización, con la consiguiente afectación a los usuarios.

Además, el agotamiento de los recursos de memoria principal, podrían afectar significativamente, en un futuro no muy lejano, las capacidades de creación de nuevas máquinas virtuales que cada vez consumen más recursos de memoria.

A través del suministro del servidor objeto de este expediente, el sistema queda preparado para evitar la necesidad de detener máquinas virtuales y, por tanto, servicios, si uno de los servidores de virtualización no está operativo. A su vez, el número de máquinas virtuales que pueden ser creadas, así como su dimensionamiento, aumenta considerablemente, preparando el centro para nuevos proyectos que requerirán más recursos.

2.2.2 Requisitos técnicos

Se requiere un servidor para ampliar el clúster de virtualización (con VMware vSphere), con las siguientes características:

- Servidor enracable, con máximo de 2 U
- Un procesador de Intel Xeon Gold de 24 cores y frecuencia básica mínima de 2,9 GHz (o equivalente)
- 512 GB RAM, 5600 MT/s, en módulos de al menos 64 GB.
- Tarjeta de arranque con dos discos de 480 GB SSD NVMe en RAID 1, para el hipervisor.

- Seis ventiladores de alto rendimiento
- Doble fuente de alimentación (redundante). Intercambiable en caliente, Titanium.
- Cuatro puertos de red ethernet 10 Gb BaseT.
- Dos puertos de red ethernet 1 Gb BaseT.
- Tarjeta de gestión remota con las siguientes funcionalidades:
  - Control remoto y medios virtuales:
    - La solución deberá proporcionar consola KVM basada en HTML5 (sin plugins) con soporte de teclado/ratón, portapapeles y colaboración multiusuario concurrente.
    - Debe permitir medios virtuales (montar ISO/IMG, carpetas remotas y discos) para instalación y rescate sin agentes.
    - Debe operar independientemente del sistema operativo y ser accesible cuando el servidor esté apagado o con el SO inoperativo (siempre que haya alimentación AC).
  - Acceso y conectividad de gestión.
    - Puerto Ethernet dedicado de gestión independiente de los puertos de datos.
    - Acceso local de mantenimiento por USB (modo “direct”) para configurar/recuperar el BMC sin red, y aplicación móvil opcional para operación cercana (BLE/Wi-Fi o equivalente).
    - Soporte de IPv4/IPv6, VLAN de gestión, NTP, DNS, proxy y out-of-band vía red de gestión segregada.
  - Seguridad y cumplimiento
    - RBAC con perfiles y permisos granulares; integración con directorio corporativo (LDAP/AD) y SSO.
    - Autenticación multifactor (2FA); bloqueo por IP, captcha/antifuerza bruta y banners de advertencia configurables.
    - TLS 1.2/1.3 con certificados personalizados (CA interna), desactivación de cifrados débiles y cumplimiento de buenas prácticas criptográficas.
    - Firmware firmado, cadena de confianza, secure boot del BMC y modo de bloqueo para impedir cambios no autorizados.
    - Exportación de logs a syslog (idealmente con TLS), sellado de eventos y trazabilidad de auditoría.
  - Despliegue y configuración
    - Zero-Touch Provisioning mediante perfiles de configuración exportables / importables (textuales o JSON/YAML), aplicables de forma masiva.
    - Instalación del sistema operativo sin agentes usando medios virtuales/archivos remotos y asistentes de aprovisionamiento.
    - Plantillas para BIOS/RAID/firmware/redes aplicables por lote y con verificación de cumplimiento.
  - Actualización y mantenimiento

- Actualización remota del BMC/BIOS/firmware de dispositivos con firma/verificación, programación de ventanas, y rollback ante fallo.
- Posibilidad de repositorios internos de parches/matrices validadas y comprobación de compliance.

- Monitorización y alertas fuera de banda
  - Telemetría OOB de salud de hardware (CPU, memoria, discos, PSU, ventiladores, temperaturas, sensores, tarjetas de red, controladoras).
  - Alertas configurables por correo/SNMP/WEBHOOK y umbrales; exportación de inventario y estado.
  - Captura de pantalla del crash/boot y acceso a SEL/Lifecycle logs para diagnóstico.
- Energía y térmica
  - Lecturas de consumo eléctrico en tiempo real/histórico, umbrales/alertas y gráficas.
  - Power capping por servidor/perfil y políticas térmicas para optimizar ruido/energía/rendimiento.
  - Integración con herramientas de gestión de energía de CPD (vía API estándar).
- Gestión "uno-a-muchos":
  - Consola de gestión grupal nativa para operar cientos de nodos sin necesidad de agentes (descubrir, etiquetar, aplicar perfiles, actualizar por lote).
  - Aprobación/flujo de cambios y vista de cumplimiento frente a una línea base.
- Interfaces y automatización:
  - API Redfish (REST) completa para todas las funciones clave; utilidades CLI remotas (p. ej., RACADM-like o equivalente), IPMI y SNMP para compatibilidad heredada.
  - Ejemplos/SDK para automatización (Ansible/Terraform/PowerShell/Python) y documentación de endpoints.
- Requisitos físicos y operativos del BMC
  - BMC integrado con memoria de lifecycle persistente, alimentación mientras el chasis reciba AC y recuperación autónoma.
  - Aislamiento de la interfaz de gestión respecto a la de producción; soporte de listas de control (permitir/denegar) y 802.1X (si aplica).
- Licenciamiento y derechos de uso
  - Incluir la edición/activación que habilite KVM HTML5 + medios virtuales + gestión grupal + seguridad avanzada desde el día 0 del proyecto.
  - Licencias perpetuas o de duración mínima 5 años, transferibles al hardware sustituto en caso de RMA.
- Soporte y ciclo de vida:
  - Soporte 24x7 para el BMC y sus actualizaciones; boletines de seguridad, CVEs y roadmap de firmware.
  - Matriz de interoperabilidad con los sistemas operativos y hypervisors propuestos.

Financiado por la Unión Europea NextGenerationEU
MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

- Otros requerimientos:
  - Telemetría continua/streaming vía Redfish Events o suscripción, exportable a SIEM/observabilidad.
  - Integración móvil con inventario/etiquetado por near-field (BLE/Wi-Fi) y QR en frontal.
  - Panel de sostenibilidad (kWh, CO_2 estimado, KPIs) exportable.

- Licencia iDRAC Enterprise para la herramienta de gestión Dell OpenManage ya en uso en la organización.
- Kit de enracado.
- Brazo de gestión de cableado
- Debe poder integrarse con la herramienta Dell OpenManage ya en uso en la organización.

2.3 Suministro para la ampliación de la capacidad de almacenamiento del sistema de virtualización

El adjudicatario deberá suministrar un sistema de almacenamiento de acuerdo a los requerimientos establecidos por el CAHA y manteniendo una compatibilidad absoluta con la instalación existente. Deberá, así mismo, suministrar cualquier material necesario para su correcta instalación y funcionamiento.

2.3.1 Contexto actual

La capacidad de almacenamiento con la que cuenta actualmente el sistema de virtualización empieza a verse sometida al estrés de la necesidad de crear nuevas máquinas virtuales con discos de cada vez mayor capacidad. A diferencia de la granja de servidores, el actual sistema de almacenamiento no permite más ampliaciones, lo que puede llegar a impedir la creación en el futuro de nuevas máquinas y servidores virtuales y no poder dar soporte virtualizado (con todas las ventajas que esto supone) a nuevos proyectos que puedan requerir de una gran capacidad de almacenamiento. Adicionalmente, las cabinas de almacenamiento son los elementos más costosos de mantener una vez finalizado su periodo de mantenimiento por parte del proveedor, ya que cuenta con varios discos de alta capacidad y rendimiento repartidos en cinco cabinas con sistemas duplicados de tensión o procesamiento.

Desde el punto de vista operativo, dejar estos sistemas sin un mantenimiento apropiado y sin un acceso a piezas de sustitución en plazos razonables, supondría un riesgo cierto para el funcionamiento del observatorio, por lo que este mantenimiento anual de las cabinas de almacenamiento (que ya están fuera de garantía) es estrictamente necesario mientras no se sustituyan.

La cabina o cabinas de almacenamiento que suministre el adjudicatario, deberán ser totalmente compatibles con el sistema de virtualización del observatorio, y, además, deberán poder integrarse en el mismo sin necesidad de parada alguna y funcionando en paralelo a las cabinas que actualmente están operativas. Este nuevo sistema de cabinas deberá ser presentado a la

virtualización como un almacenamiento nuevo y adicional al que actualmente está funcionando, y las máquinas que en este momento trabajan en el almacenamiento antiguo deberán poder migrarse al nuevo almacenamiento de forma transparente, desde el propio vSphere y sin parada alguna.

2.3.2 Requisitos generales

Se requiere un sistema de almacenamiento nuevo que presente las siguientes características mínimas:

- Capacidad efectiva: 874 TB efectivos:
  - En un RAID de, al menos, doble paridad.
  - Dejando un disco para 'spare'.
  - Esta capacidad, calculada contando con mecanismos de optimización como compresión y/o deduplicación.
  - En caso de que la capacidad efectiva se alcance usando mecanismos de eficiencia (deduplicación, compresión, etc), el fabricante debe comprometerse por escrito, en contrato enviado al cliente, a suministrar las ampliaciones necesarias del sistema para llegar al nivel de eficiencia comprometido en la oferta.
- Capacidad neta usable: 291 TB
  - Antes de aplicar mecanismos de optimización y/o deduplicación.
  - En un RAID de, al menos, doble paridad.
  - Dejando un disco para 'spare'

2.3.3 Requisitos físicos

- Los discos deben ser NVMe SSD, de tecnología QLC (o superior) y deben permitir encriptación AES-256
- Alta disponibilidad y confiabilidad: Se podrá implementar una arquitectura de almacenamiento con alta disponibilidad (HA), evitando puntos únicos de fallo. La solución debe asegurar continuidad operativa incluso ante fallos de componentes, gracias a controladoras redundantes en modo activo-activo y mecanismos robustos de protección de datos.
- 24 slots internos para discos.
- Posibilidad de crecer hasta 72 discos sin necesidad de añadir controladoras adicionales.
- Interfaces de red: 8 x 10 Gb BaseT (4 en cada controladora).
- Soporte a conectividad 64Gb, 32Gb y 16 Gb para protocolo Fibre Channel y NVMe/FC.
- Soporte a conectividad 100GbE, 40GbE, 25 GbE y 10GbE para Ethernet (NAS, S3, iSCSI y NVMe/TCP).
- Latencia: inferior a 4 milisegundos.
- Disponibilidad de al menos 99,9999% certificada por alguna empresa consultora externa.
- Altura: 2U.

- 128 GB de RAM.
- Procesadores Intel con al menos 20 CPU cores en la pareja HA.
- Doble fuente de alimentación extraíble en caliente.
- Posibilidad de extracción de componentes en caliente (ventiladores, fuentes de alimentación, discos, cambio de controladoras...).
- Deberá disponer de baterías para caso de fallo de corriente, de forma que, ante el peor de los escenarios, se dote de tiempo suficiente para pasar los datos en memoria caché o temporal a espacio de almacenamiento no volátil.
- Fuentes de alimentación con certificación 80 PLUS Titanium con una eficiencia energética superior al 95%

2.3.4 Requisitos funcionales

- Deberá tener capacidad de escalar hasta 8 controladoras (4 sistemas de almacenamiento) en el mismo clúster:
  - Capacidad para configurar un clúster de almacenamiento con otros modelos de almacenamiento del mismo fabricante.
  - Los sistemas de almacenamiento en el posible clúster deberán poder tener discos de otras tecnologías, con opciones como mínimo: SSD TLC, SSD QLC, SAS y/o NL-SAS).
- Protocolos: Se deberá prestar los servicios de SAN (FC, iSCSI, NVMe-oF, NVMe-TCP), NAS (NFS, pNFS y CIFs) y Objeto (S3) a la vez desde ambas controladoras, sobre sus puertos y de manera nativa, sin uso de gateways, software externo, ni servicios basados en contenedores que corran en el sistema de almacenamiento. Se podrán compartir volúmenes SAN, NAS y Objeto entre las controladoras y reasignar espacio entre ellas para los diferentes servicios y protocolos.
- NFS sobre RDMA: deberá permitir la copia de datos de manera directa entre la memoria del sistema de almacenamiento y la memoria del host, para los protocolos NFSv3, NFSv4.0 y NFSv4.1.
- NFS trunking: trunking de sesiones abriendo múltiples conexiones entre la cabina de almacenamiento y los clientes para poder incrementar el rendimiento para NFSv4.1.
- Gestión avanzada y escalabilidad a largo plazo: Deberá disponer de un software de gestión de almacenamiento integral que ofrezca funcionalidades avanzadas (administración centralizada, calidad de servicio QoS, snapshots/instantáneas, replicación síncrona y asíncrona) y que permita escalabilidad tanto vertical (añadiendo capacidad o controladoras a la solución) como horizontal (añadiendo nodos o sistemas adicionales) para acomodar el crecimiento futuro de los datos.
- Deberá permitir replicación de datos nativa entre sistemas de almacenamiento, en modo asíncrono y síncrono, sin rehidratación del dato manteniendo las eficiencias de almacenamiento obtenidas gracias a las funcionalidades de deduplicación, compactación y compresión en origen e independiente del protocolo utilizado. Replicación cifrada mínimo TLS 1.2 AES-256 GCM.

- Deberá permitir replicación Síncrona: Capacidad de crear una replicación síncrona entre CPDs, en modo activo/activo para los protocolos de bloque (SAN), que proporciona conmutación de servicio automática entre CPDs sin pérdida de datos (RPO=0) ni pérdida de servicio (RTO=0) para las aplicaciones.
- Espacio global de nombres único: la solución de almacenamiento deberá poder desplegar tanto en la propia cabina como en otra cabinas de almacenamiento del fabricante, bien sea en modo on-premise como nube pública, un espacio de nombres único (global Namespace), de manera que sea posible acceder a un repositorio de datos centralizado de manera simultánea para protocolos NAS (NFS y SMB) tanto en escritura como en lectura, desde cualquiera de las cabinas que compongan dicho espacio de nombres único.
- Snapshot. Deberá tener posibilidad de copias instantáneas, con tecnología Redirect-on-write para no impactar en rendimiento. Deben poderse realizar en menos de 1 segundo, independientemente del tamaño del volumen o del nivel de actividad del sistema de almacenamiento y ocupar solamente los cambios realizados después de su creación. Accediendo a las carpetas compartidas pertenecientes a las copias instantáneas deberá ser factible restaurar posibles ficheros borrados. Dichos snapshots han de ser de solo lectura, inmutables y admitir la posibilidad de aplicar WORM de forma granular, estableciendo un periodo de retención a nivel de snapshot durante el cual permanezcan indelebles, siendo completamente imposible su eliminación durante dicho periodo de retención desde la consola de administración del almacenamiento.
- Snapshot en destino. Deberá tener posibilidad de copias instantáneas en destino de los volúmenes replicados, con distintas retenciones que las copias instantáneas de los volúmenes originales. Accediendo a las carpetas compartidas pertenecientes a las copias instantáneas realizadas a partir las réplicas sería factible restaurar posibles ficheros borrados.
- Planificación de los Snapshot. Tanto en origen como en destino, se deberá poder dejar planificada la creación de snapshot indicando frecuencia y número de copias: por ejemplo, hasta 4 copias cada 6 horas, hasta 10 copias una vez al día, hasta 3 copias una vez al mes. Además, en la configuración de los snapshot deberá poderse indicar un tamaño máximo a partir del cual se borrarían los snapshot más antiguos.
- Thin Provisioning. Posibilidad de ofrecer a los usuarios más espacio del que realmente existe en las cabinas. El espacio se debe ir consumiendo a medida que se vayan llenando las carpetas compartidas con ficheros, asimismo, se debe recuperar el espacio cuando se borren ficheros. Esto es, el espacio libre de la cabina debe ser común para las diferentes carpetas compartidas definidas de este modo y dichas carpetas (así como los contenedores donde se ubicasen) deben poder ampliarse en caliente y sin pérdida de servicio hasta consumir el espacio libre.
- Permitirá la migración de carpetas en caliente. Si por la arquitectura de la solución (por ejemplo, en función del tipo de RAID o tipo de Disco), las carpetas compartidas se ubicasen dentro de algún tipo de contenedor físico o lógico, se debe ofertar la migración de carpetas compartidas de un contenedor a otro, todo esto en caliente y sin pérdida de servicio. Estas

migraciones de carpetas en caliente se entienden siempre dentro del mismo servicio de ficheros.

- Eficiencia y optimización del almacenamiento: podrá reducir el espacio requerido para datos mediante deduplicación, compresión y aprovisionamiento delgado (thin provisioning), garantizando que la capacidad efectiva se logre con la menor cantidad de soporte físico posible sin sacrificar rendimiento.
- Deduplicación: Las cabinas tendrán capacidad de presentar una solución de "deduplicación" de manera INLINE para discos SSD y post-proceso para el resto de discos.
- Compresión: Las cabinas tendrán capacidad de presentar una solución de "Compresión" de manera INLINE para discos SSD y post-proceso para el resto de discos.
- Compactación: Las cabinas tendrán capacidad de presentar una solución de "compactación" de manera INLINE para discos SSD y post-proceso para el resto de discos.
- Logs de auditoria: Tendrá capacidad de activar la recopilación de logs de acceso a los ficheros de determinadas carpetas compartidas.
- Seguridad/Cifrado: dará respuesta a los siguientes requerimientos:
  - Capacidad de Cifrado FIPS 140-3 a nivel software para la información contenida en volúmenes (SAN, NAS y S3), decidiendo que volúmenes se cifran y cuáles no.
  - Capacidad de permitir Two Factor Authentication (2FA) para conexiones SSH y CLI
  - Permitir el uso de certificados para comunicaciones con REST API
  - Permitir IPsec data-in-flight encryption para todo el tráfico IP
  - NFS sobre TLS
  - LDAP sobre TLS
  - S3 sobre TLS/SSL por defecto
  - Permitir el uso de HTTPS como protocolo de transporte predeterminado para enviar mensajes de "call home"
  - Que la replicación proporcione soporte cifrado TLS 1.2 AES-256 GCM mediante una clave precompartida (PSK).
  - Debe soportar RBAC (Role Based Access Control) donde diferentes administradores tienen diferentes niveles de acceso al sistema.
  - Que el sistema tenga un firewall interno para restringir el tráfico de gestión de la cabina.
  - El sistema debe ser contar con la certificación CSfC (Commercial Solutions for Classified) para funcionalidades de data-at-rest (DAR)
- Clonado: Deberá tener capacidad de Clonar datos de NAS y SAN sin ocupar espacio hasta que se modifiquen los clones.
- WORM. Deberá tener capacidad de realizar WORM a ciertos ficheros o volúmenes de datos para que no puedan ser modificados ni borrados durante un periodo de tiempo establecido., en modos Enterprise y compliance
- WORM S3. Deberá soportar object lock en modalidades Governance y Compliance

- DevOps: El sistema ha de ser capaz de proporcionar almacenamiento persistente de código abierto a través de un orquestador de tipo open-source para Kubernetes, OpenShift, Docker y Rancher. El orquestador debe permitir funcionalidades como thin provisioning, near-instantaneous clones y snapshots, workload isolation, entre otras. También se deberá disponer de módulos certificados por Ansible para la automatización de las actividades de gestión del almacenamiento.
- Integración API Rest: El sistema de almacenamiento debe tener capacidades de integración vía API Rest para obtener información a nivel de Servicios de ficheros CIFs y NFS.
- Copias de seguridad: la solución deberá incluir un software de copias de seguridad. Este permitirá realizar copias de seguridad consistentes a nivel de aplicación basadas en tecnología snapshot para proteger entornos de VMWare, Oracle, Windows Server, SAP HANA, SQL Server y MongoDB.
- Volumen Único: El sistema de almacenamiento deberá ser capaz de poder crear un único volumen CIFs o NFS, con un único punto de montaje, que utilice todas las controladoras y recursos de cada CPD, permitiendo crear un único volumen del tamaño de toda la capacidad que pueda gestionar la cabina, varios PiB de información.
- Deberá tener capacidad de crear RAID de doble y triple paridad.
- Deberá permitir actualizaciones no disruptivas de todos los componentes.
- Calidad de Servicio: Deberá tener posibilidad de ofrecer QoS adaptativo (IOPs/TBs) en función de la carga de los volúmenes y a los recursos disponibles de las cabinas para SAN y NAS, garantizando el rendimiento de las aplicaciones que se ejecuten dentro del sistema de almacenamiento. Con capacidad de limitar anchos de banda de LUNs o volúmenes y también de garantizar la cantidad de IOPS.
- Deberá contar con un servicio de AutoSupport, conectado al centro de soporte del fabricante del software de almacenamiento, para proporcionar una visibilidad simple y segura sobre la salud de los sistemas desde un portal web que se le proporcionará al cliente. Deberá trabajar continuamente en segundo plano para descubrir posibles problemas y proponer proactivamente optimizaciones en el entorno del cliente. Las evaluaciones continuas de riesgos, las alertas predictivas, la orientación prescriptiva y las acciones automatizadas ayudarán a prevenir problemas antes de que ocurran, lo que conduce a una mayor salud del sistema y una mayor disponibilidad de este.
- Deberá tener capacidad de hacer tiering de los bloques fríos a un almacenamiento externo vía S3.
- Deberá tener capacidad de ubicar los snapshot únicamente en un almacenamiento externo vía S3.
- Multidominio de Directorio Activo: Los servicios de ficheros ofrecidos han de poderse integrar con el Directorio Activo de Microsoft. La cabina ha de permitir que cada servicio de ficheros pueda estar en un Directorio Activo diferente.
- Cuotas de espacio en disco: La cabina deberá ser capaz de gestionar cuotas de espacio de ocupación en disco por carpeta compartida, de manera que cuando dicha carpeta compartida

llegue a la capacidad indicada no permita seguir añadiendo más contenido a esa carpeta. La modificación de cuotas ha de poderse realizar en caliente.

- Tipos de ficheros: El almacenamiento debe tener un sistema de notificación que permita a los administradores impedir que los usuarios finales almacenen archivos no deseados para SMB y NFSv3 y v4.x. Esta función debe bloquear los archivos basándose en la extensión de los ficheros.
- Protección Ransomware autónoma, dentro del almacenamiento sin necesidad de elementos externos, que analiza las cargas NAS (NFS y SMB) para de manera proactiva detectar y alertas sobre actividad anormal que podría indicar un ataque ransomware. El mecanismo de detección de Ransomware ha de actuar frente a ataques de denegación de servicio por cifrado de datos (atacantes bloquean el acceso hasta recibir un pago de rescate). El mecanismo debe permitir:
  - Identificación de los datos NAS como cifrados o texto plano
  - Analítica de detección de:
    - Datos de alta entropía (una evaluación de la aleatoriedad del dato dentro de un fichero)
    - Un aumento anormal de la actividad de un volumen de datos con cifrado
    - Una extensión de fichero que no sea conforme con las extensiones normalmente utilizadas en el sistema de ficheros.
  - Cuando un ataque sea detectado, deben crearse copias de Snapshot inmutables, además de las ya existentes partes de la programación de copias de Snapshot de los volúmenes de ficheros
  - Dichas copias de Snapshot además de inmutables deben permanecer bloqueadas frente a borrado, de esta manera se obtiene un punto de recuperación muy cercano al evento.
  - Dichas copias de Snapshot no se pueden eliminar hasta que el administrador del sistema de almacenamiento proporcione respuesta humana al mecanismo de Machine Learning, bien identificando el ataque como real o falso positivo.
  - La protección Anti-Ransomware del sistema debe tener una precisión en la detección de al menos un 99% auditado por una entidad externa al fabricante.
- Deberá contemplar el acceso de control de acceso a los sistemas de ficheros mediante mecanismos de filtrado de extensiones, de esta manera se crean reglas o listas de acceso permitiendo o denegando el acceso desde el exterior a determinadas extensiones frente a determinadas acciones (renombrar, crear, reescribir, leer…). Se trata de una primera barrera de protección frente a ransomware para aquellos tipos de ataque que además de cifrar el dato modifiquen la extensión del fichero.
- Para la funcionalidad NAS, deberá poderse configurar un sistema de cache en un tercer almacenamiento -no necesariamente del mismo modelo- en una posible ubicación remota para acceder en esta de forma local para lecturas y escrituras a los ficheros de este almacenamiento.
- Verificación de acciones de administrador de almacenamiento, funcionalidad que asegura que determinadas acciones administrativas tales como borrado de volúmenes de datos o copias de

Snapshot solo puedan ser ejecutadas tras la aprobación de administradores designados. Esto previene de usuarios administradores comprometidos, maliciosos o inexperimentados que puedan realizar cambios indeseables o borrados de datos. Dicha funcionalidad deberá permitir:
  - Definición de uno o más grupos de administradores con poderes de aprobación / veto.
  - Set de operaciones protegidas o comandos
  - Motor de reglas para identificar y controlar la ejecución de acciones protegidas
  - Aparte ha de notificar frente a acciones realizadas a los grupos de administradores vía alertas de correo electrónico (haciendo uso de eventos EMS) cuando se cree una petición, se apruebe, se vete o se ejecute.

- Se incluirán todas las licencias necesarias para el uso sin limitaciones de todas las funcionalidades requeridas.
- Integración con Entornos de Virtualización y Sistemas Operativos: El almacenamiento propuesto debe ser compatible con las plataformas de virtualización y contenedores en uso, facilitando su integración en entornos existentes de la organización. Específicamente, se requiere compatibilidad y herramientas de integración con VMware vSphere (por ejemplo, soporte de VAAI, o plugins de VMware para gestión del storage), compatibilidad con hipervisores KVM, y soporte para entornos de orquestación de contenedores Kubernetes (por ejemplo, mediante drivers CSI – Container Storage Interface). Asimismo, deberá garantizarse el soporte para su uso con sistemas operativos Linux (distros comunes, y en especial OpenSuSE) en la presentación de volúmenes y compartidos, incluyendo soporte de multipath IO en Linux para conexiones iSCSI/FC.
- Integración con Servicios de Nube Pública: La solución debe ofrecer mecanismos de integración con al menos tres plataformas de nube pública líderes con presencia en Europa de cara al cumplimiento de normativas tipo GDPR. La replicación de los datos se debe hacer con los datos deduplicados y comprimidos y manteniendo las deduplicación y compresión en destino sin necesidad de rehidratar el dato. Esta integración debe incluir funcionalidades como: replicación de datos hacia la nube, tiering de datos fríos a almacenamiento en la nube, capacidad de sincronización o failover hacia instancias de almacenamiento en nube pública, o disponibilidad de una interfaz de gestión unificada para entornos híbridos (in-situ y en la nube. Aunque no se exige nombrar proveedores específicos, se valorará que la solución pueda interoperar con servicios equivalentes a los de los principales proveedores globales de nube (por ej., funcionalidades compatibles con AWS, Azure, Google Cloud, IBM Cloud, etc., sin mencionarlos explícitamente).

2.4 Suministro licencias de VMware vSphere

Forma parte del alcance de este expediente **un (1)** año de suscripción de las licencias de VMware vSphere Standard para todos los Cores del nuevo servidor de virtualización (ver apartado 2.2.2) objeto de esta licitación.

Durante la vigencia de esta suscripción, CAHA podrá tener acceso a la versión en operación más reciente por el fabricante, así como los parches liberados por el fabricante.

2.5 Suministro licenciamiento de Nakivo Backup & Recovery

El sistema actual en funcionamiento ya dispone de Nakivo Backup & Recovery para la realización de copias de seguridad.

Forma parte del alcance de este expediente un (1) año de suscripción del software Nakivo Backup & Recovery necesarias para ampliar esta instalación existente con el nuevo servidor de virtualización que será adquirido en esta licitación.

Durante la vigencia de esta suscripción, CAHA podrá tener acceso a la versión en operación más reciente por el fabricante, así como los parches liberados por el fabricante.

3 Garantías

La garantía ofertada para todo el equipamiento físico suministrado será de un mínimo de tres (3) años de duración, valorándose una ampliación de este plazo[1].

Los requerimientos asociados a la garantía exigida son:

- Debe ser garantía ofrecida directamente por el fabricante del equipo.
- Durante el plazo de garantía, el contratista garantizará la plena conformidad y operatividad del servidor y la cabina de discos. A tal efecto, asumirá íntegramente la gestión de RMA con los fabricantes, incluyendo apertura y seguimiento de casos, suministro de repuestos, mano de obra y desplazamientos on-site, embalajes, portes, aduanas y cualesquiera otros costes asociados, sin intervención del órgano de contratación.
- El contratista será único interlocutor para incidencias, proporcionando atención con tiempos máximos NBD para restablecimiento/sustitución.
- El contratista dará de alta las garantías a nombre del órgano de contratación y aportará acreditación documental.
- En el caso de la cabina de almacenamiento (ver apartado 2.3), deberá incluir soporte directo con el fabricante (niveles L1, L2 y L3). No se admitirán soportes de partners ni de OEMizadores.
- Adicional a las licencias y soporte del fabricante, forma parte del alcance de la garantía una bolsa de 100 horas anuales de asistencia técnica al CAHA para las licencias/suscripciones de VMware y Nakivo durante los años de vigencia de la garantía. La disponibilidad de este servicio de soporte será de lunes a viernes de 8:00 a 18:00.

El licitador expondrá en la Memoria técnica (ver apartado 6.3) las condiciones en las que prestará la garantía.

[1] El licitador no incluirá en la Memoria Técnica (apartado 6.3) ningún dato que dé lugar a conocer (ni directamente ni mediante inferencia) su propuesta para el criterio de adjudicación sujeto a fórmula "Ampliación del periodo de garantía".

4 Duración del contrato

El plazo máximo de duración del contrato es de **OCHO (8) SEMANAS**, a contar desde la fecha de formalización del mismo.

Este plazo incluye tanto la fabricación y preparación de la maquinaria como su transporte e instalación en las dependencias del CAHA.

5 Lugar de suministro

El suministro debe ser entregado en el Observatorio de Calar Alto, con dirección: Centro Astronómico Hispano en Andalucía, A.I.E. Compj. Observatorio Astronómico de Calar Alto, s/n. Sierra de los Filabres 04550 - Gérgal (Almería).

6 Oferta técnica

6.1 Aspectos generales

En relación con la preparación de la oferta técnica, las empresas licitadoras deberán tener en cuenta lo siguiente:

La estructura y contenido de la oferta técnica en general y de la memoria técnica en particular, debe ajustarse estrictamente a lo establecido en sus respectivos apartados. Toda información que no se encuentre dentro de dicha estructura no se tendrá en cuenta, salvo que los pliegos establezcan lo contrario.

La oferta técnica incluirá, en su caso, anexos con información relacionada con el contenido de la memoria técnica. La inclusión de anexos será opcional para las empresas licitadoras excepto en los casos en los que los pliegos establezcan la obligatoriedad de incluir alguno. La información de los anexos no intervendrá en la valoración de los criterios de adjudicación y, por lo tanto, su contenido será complementario y/o servirá como elemento de verificación de lo incluido en la memoria técnica. No obstante, la no inclusión de anexos que los pliegos establezcan como obligatorios será motivo de exclusión de la oferta.

La estructura y el contenido de la memoria técnica se corresponde uno a uno con los 'aspectos a valorar' de los criterios de adjudicación cuantificables mediante un juicio de valor. Con el fin de incluir en cada apartado la información adecuada, se recomienda la lectura de la metodología de valoración de este tipo de criterios incluida en los pliegos.

La información que se incluya en la oferta técnica no debe contener ningún dato o valor referido a los criterios evaluables mediante fórmulas, ni información que permita deducirlos ya que, de ser así, la propuesta en su conjunto se excluirá automáticamente del proceso de licitación.

Sobre la memoria técnica:

En el caso de establecerse limitaciones de extensión de la memoria técnica, el contenido de las páginas que excedan dicha extensión no será tenido en cuenta a la hora de la valoración de los criterios sujetos a un juicio de valor y, en consecuencia, los 'aspectos a valorar' afectados se puntuarán con 0 puntos.

Se valorará la concreción en la exposición de las propuestas. El licitador deberá evitar la inclusión de información redundante, innecesaria o no relevante, incluso cumpliendo con la limitación de extensión expuesta anteriormente.

La mesa de contratación podrá exigir a los licitadores documentación justificativa que acredite cualquier aspecto incluido en la oferta técnica, así como precisiones o aclaraciones sobre las ofertas presentadas o información complementaria relativa a ellas, si bien las respuestas no podrán suponer una modificación de los elementos fundamentales de la oferta.

6.2 Contenido de la oferta técnica

La oferta técnica estará formada por un único documento (fichero) y constará obligatoriamente de los siguientes apartados:

1. Portada en la que se identifique claramente el título y el número de expediente al que corresponde la oferta.
2. Índice de la oferta técnica.
3. Acatamiento de los pliegos e identificación de la empresa licitadora en una página con la siguiente información:
    a. Párrafo en el que la empresa licitadora exprese el acatamiento de la totalidad de lo establecido en los pliegos y en el que se declare la veracidad de la información incluida en la oferta técnica.
    b. Cuadro en el que se incluyan los datos de licitador y los de la persona de contacto.
4. Memoria técnica, que contiene de forma ordenada todos los criterios cuya valoración está sujeta a un juicio de valor:

6.3 Memoria técnica

La Memoria Técnica deberá ajustarse obligatoriamente a la siguiente estructura y contenido:

CAPÍTULO		APARTADO		SUBAPARTADO	
1	Solución propuesta	1	Enfoque para ejecutar la garantía de los equipos	a)	Herramientas y procedimientos mediante las que el licitador prestará el servicio de garantía.
				b)	Certificaciones del equipo del licitador en las tecnologías ofertadas tanto del servidor como de la Cabina de disco
				a)	Modalidades de prestación: disponibilidad para la prestación in situ en caso de ser necesario por razones de urgencia o por imposibilidad de resolución mediante soporte remoto.

6.4 Limitaciones de extensión de la oferta técnica

Se establecen las siguientes limitaciones en la extensión de la memoria técnica:

- Memoria Técnica: 10 páginas

En ambos casos las páginas se ajustarán a las siguientes características:

- Tamaño hoja: A4
- Tipo letra: Arial o tipo con tamaño de letra equivalente
- Tamaño letra mínimo: 11 ppp
- Márgenes mínimos: 2 cm a cada borde
- Interlineado mínimo: sencillo