Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

INFRAESTRUCTURA DE VIRTUALIZACIÓN DE LA UNIVERSIDAD DE ALCALÁ

PLIEGO DE PRESCRIPCIONES TÉCNICAS

1. OBJETO DEL CONTRATO

El objeto del contrato es el suministro, la instalación y la configuración de infraestructura tecnológica para el entorno de virtualización de la Universidad de Alcalá (en adelante UAH), así como la migración a este entorno de los sistemas y servicios virtualizados en la infraestructura de virtualización actual.

2. CARACTERÍSTICAS TÉCNICAS

Las características técnicas del equipamiento objeto de este pliego son las siguientes.

2.1. Elementos primarios

2.1.1. Descripción general

El equipamiento deberá conformar en su núcleo principal una solución de infraestructura híper-convergente (HCI) donde cada nodo es capaz de proporcionar recursos de computación, red y almacenamiento y agregarlos al conjunto del sistema.

La solución de Hiper-Convergencia deberá estar en su conjunto certificada tanto por el fabricante de la misma como por el del hipervisor.

El sistema presentado deberá certificar que soporta el hipervisor que actualmente utilizan los Servicios Informáticos de la UAH, esto es, VMware vSphere.

La solución debe constituirse y considerarse como un único producto compuesto por nodos híper-convergentes, que incluyan la virtualización del hardware incluyendo la provisión en modo *software-defined* a través del hipervisor del proceso, el almacenamiento y la red.

De acuerdo con el punto anterior, el mantenimiento y las actualizaciones de la solución deberán ser proporcionados de forma unificada a través de un único contrato de soporte que cubrirá (de extremo a extremo) todo el hardware y el software de la plataforma (incluyendo el hipervisor).

La plataforma debe permitir la aplicación de buenas prácticas recomendadas respecto al hipervisor, incluyendo niveles de resiliencia, factores de protección, tolerancia a fallos y equilibrado de carga a todos los niveles, sin tolerar pérdida de datos y con respuesta automática ante la contingencia. Una vez firmado el contrato, el adjudicatario deberá remitir a los Servicios Informáticos la documentación descriptiva de las buenas prácticas recomendadas por el fabricante.

El sistema debe integrarse perfectamente en la experiencia de software del entorno que actualmente utilizan los Servicios Informáticos de la UAH, basada en VMware:

- Ecosistema vSphere de configuraciones y soluciones compatibles.
- Arquitecturas de referencia.
- Herramientas M&O familiares a los administradores de VMware.

La solución debe ser flexible para abordar una amplia gama de aplicaciones y servicios de las organizaciones, incluyendo tanto la gestión de datos estructurados (como bases de datos)

como datos no estructurados (correos electrónicos, documentos y vídeo…) o entornos de escritorio virtual / plataformas de computación, entre otros ejemplos.

2.1.2. Características técnicas

La solución global debe ofrecer al menos de 85 TiB (terabytes netos) disponibles de almacenamiento, basados al 100% en tecnología de discos flash y asumiendo un FTT=1 (*failures to tolerate*), RAID 5 y reserva de espacio del 30%.

En la descripción técnica se describirá el gestor de almacenamiento SDS (Software Define Storage) y la plataforma hardware subyacente. Si se emplean mecanismos de eficiencia (por ejemplo, compresión y/o deduplicación de datos) se describirán, así como los cálculos y asunciones que hayan sido tomadas para llegar al espacio disponible.

Se detallará la conectividad interna y externa de los nodos, así como los mecanismos de discriminación de tráfico interno de la plataforma del tráfico de acceso y servicio a los usuarios.

El hipervisor debe incluir *switches* virtuales distribuidos de vSphere para gestionar las configuraciones de red como una sola entidad.

La solución debe ofrecer un sistema de almacenamiento que se gestione a través de políticas (en lugar de grupos RAID / seLUNs / Sistemas de ficheros) que permitan asignar directamente el nivel de rendimiento y la calidad del servicio y protección de datos requeridos, con una granularidad de VM. Así mismo, se deben proporcionar controles de calidad de servicio (QoS) por VM, todo ello con posibilidad de que dichas configuraciones a nivel de VM (objeto) se puedan hacer dinámicamente.

La solución debe soportar los estándares PCI para maximizar la seguridad de la información y minimizar los riesgos en caso de caída, pérdida / corrupción de datos, acceso no autorizado o fallos de cumplimiento de los niveles y garantías de servicio.

La plataforma debe ser capaz de protegerse contra el fallo simultáneo de al menos 1 elemento del mismo tipo (como mínimo) sin pérdida de datos ni servicio (controlador, discos y/o nodo).

En caso de fallo de los componentes hardware que constituyan el almacenamiento, el sistema será capaz de reconstruir rápidamente los datos en la infraestructura superviviente y este proceso no generará degradación del sistema.

La solución deberá contener al menos 6 nodos, cada uno de ellos con características técnicas que deberán ser equivalentes en funcionalidad y de igual o superior capacidad a las siguientes:

- Chasis con hasta 24 discos duros de 2,5 con hasta 4 unidades NVME
- 2 procesadores tipo Intel Xeon Gold 6248R, 3.0 GHz, 24 núc./48 subpr., 10,4 GT/s, 35,75 MB de caché, Turbo, HT (205 W) o superior
- Discos flash en su totalidad, SSD SAS Read-Intensive, 12 Gb/s, unidad AG 512 2,5 conex. caliente, 1 escr/día, 7008 TB escritos, con al menos 14,31 TiB de capacidad neta, asumiendo FTT=1, RAID 5 y reserva de espacio del 30%.
- Memoria RAM de 1.152 Gb o superior, de tipo DDR4-2933, 3200 MT/s, bloque doble

- 8 SSD
- 2 Unidades AG de uso combinado NVMe Enterprise de 1,6 TB, U.2 Gen4 con portadora
- 1 Tarjeta de puerto doble 16Gb HBA de Fibre Channel, PCIe de altura completa
- 1 Tarjeta controladora BOSS con 2 tarjetas M.2 de 240 GB (RAID 1), altura completa
- 1 HBA330+ controlador adaptador, perfil bajo
- 1 Adaptador de puerto doble 10/25 GbE SFP28, PCIe de altura completa
- Guías móviles ReadyRails para montaje en rack.

2.1.3. Características y crecimiento

Deben indicarse de manera precisa y clara el espacio requerido en el CPD, su consumo energético, necesidades de refrigeración, así como otros requerimientos y/o características relevantes en relación a la instalación física y el funcionamiento de la plataforma. La solución debe implementar estrategias y tecnologías que mejoren la eficiencia energética de la plataforma.

No se aceptarán soluciones al límite de capacidades soportadas. Para comprobar este punto se deberá indicar la configuración propuesta en relación con la capacidad máxima de los nodos y del sistema en su conjunto.

No se permitirá la inclusión en la propuesta de funcionalidades en *roadmap* o que no se encuentren disponibles en versiones oficiales (Global Availability).

La solución debe ser capaz de crecer transparentemente en modo *scale-out* a través de la agregación de nodos y de modo *scale-up* a través de la posibilidad de ampliación de cada nodo ya existente (memoria, discos y/o tarjetas de red); una vez más, se indicará la capacidad de los nodos en relación con su máxima capacidad posible.

El crecimiento *scale-up* (por ejemplo, discos o memoria) no debe implicar costes añadidos de licenciamiento asociados a cualquiera de los elementos software que componen la solución de Hiper-Convergencia.

Se debe tolerar combinar nodos con diferentes capacidades (CPU, RAM, almacenamiento) y características adicionales (inclusión de GPUs) así como diferentes modelos de nodo, dentro de un mismo *cluster* de Hiper-Convergencia, para permitir un diseño ajustado a las necesidades del entorno y la adaptación a nuevas cargas de trabajo.

La solución debe permitir la posibilidad de cifrado a nivel de *storage* (capa Software Define Storage), de forma nativa y sin requerir para ello el uso de discos SED.

La solución debe permitir la posibilidad de deduplicar y comprimir en línea (*in-line*) y sin necesidad de utilizar elementos hardware adicionales para tal fin.

La solución debe ser capaz de escalar en nubes públicas permitiendo la creación de niveles de almacenamiento jerárquico, empleando para ello servicios de almacenamiento externo en la nube como Amazon, Google, Microsoft Azure, OpenStack u otros.

Todos los componentes de la solución deben ser de nueva fabricación y no se suministrarán sistemas con componentes reparados o restaurados.

Se especificará respecto al sistema y los modelos de nodos propuestos su fecha de aparición en el mercado.

2.1.4. Administración

Toda la operativa con el entorno virtual (computación, almacenamiento y red) se realizará a través de las herramientas nativas del hipervisor.

Cualquier funcionalidad que se ofrezca en el contexto de la propuesta deberá disponer de las licencias adecuadas.

La solución no debe limitar o condicionar las funcionalidades del hipervisor, como puede ser:

- El uso de *snapshots* de hipervisor, que deberán seguir siendo gestionados de forma transparente a la tecnología propuesta, de manera nativa y sin pérdida o degradación del rendimiento, a través del software de gestión centralizado.
- La capacidad de realizar clones, migraciones y asignación de recursos en el entorno virtual "en caliente", sin necesidad de utilizar software de terceros.

El almacenamiento disponible en la plataforma debe integrarse con el entorno o entornos virtuales que están ejecutándose para proveer de funcionalidades como:

- Cambio dinámico de los niveles de protección de datos.
- Deduplicación.
- Compresión.

2.1.5. Gestión

La solución debe ofrecer una experiencia de soporte integrada que proporcione una vista de los eventos hardware y software e informe del estado de la plataforma y las posibles incidencias sobre los mismos a los administradores y al fabricante de manera automática (llamada a casa). Este mecanismo de soporte remoto deberá acreditar de manera adecuada su seguridad y la posibilidad de controlar los accesos remotos del soporte del fabricante por parte del cliente.

La solución debe ofrecer un análisis predictivo de fallos con notificaciones de alerta proactivas a través de mecanismos de detección automática y alerta de comportamiento anormal en todo el entorno (incluyendo hardware - CPU, RAM, discos, tarjetas de red e interconexión -, máquinas virtuales y mecanismos de protección)

La escalabilidad de la solución propuesta deberá ser gestionada por la plataforma de gestión. El crecimiento del entorno no tiene que generar más complejidad en la gestión, debiendo automatizarse las labores de, al menos:

- Instalación del sistema.
- Actualización / parcheado de la plataforma.
- Ampliación de un nodo (adición de discos).
- Ampliación del sistema (adición de un nodo).
- Eliminación de un nodo.
- Reemplazo de elementos hardware en fallo.

- Apagado del sistema.

La plataforma de gestión deberá incluir funcionalidades de monitorización complementarias a las ofrecidas por el hipervisor, que ofrezcan las métricas necesarias para controlar el estado del entorno de virtualización y de los subsistemas hardware de forma unificada y correlacionada.

- Gráficos de consumo CPU, RAM, IOPS, del entorno completo.
- Gráficos de consumo CPU, RAM, IOPS, de cada uno de los nodos.

2.1.6. Actualización y mantenimiento

La plataforma en su conjunto deberá considerarse un único producto a la hora de realizar las actualizaciones de versiones de software, firmware y aplicaciones intrínsecas al clúster de Hiper-Convergencia incluido en propio vCenter (por ejemplo, la plataforma de gestión). El proceso de actualización ofrecerá las siguientes características:

- Existirá una matriz de compatibilidad en la que se refleje la configuración deseable de la plataforma, pública y verificada por el fabricante.
- Se generará de forma automática un paquete (según la matriz pública) que incluirá todos los elementos que se vayan a instalar durante la actualización y que se aplicarán conjuntamente.
- La configuración objetivo de cada proceso de actualización detallará la versión deseable de todos los componentes implicados en el proceso.
- La actualización se activa con un único clic y es completamente desatendida hasta su finalización.
- El proceso será sencillo y ágil, sin impacto en el entorno de producción, y ejecutándose de manera completamente automatizada de todos los elementos software y hardware de la plataforma Hiper-Convergente, una vez que el administrador ha decidido iniciar la actualización.
- La actualización podrá ser realizada sin necesidad de intervención por parte del fabricante de la plataforma.

Se deberá ofrecer un único punto de soporte con el fabricante para toda la solución. Esto es, soporte unificado de la solución completa, tanto para el hardware (nodos y sus componentes) como para el software (Hipervisor, SDS, software de gestión, etc.).

2.1.7. Otras características

Se permitirá la gestión de configuración de los Switches ToR desde la herramienta de despliegue de la solución.

Se debe permitir el uso de Erasure Code para la protección de la capa de *storage*.

La solución ofrecerá la posibilidad de configurar HCI *streched cluster* (activo/activo real) entre dos ubicaciones a distancia síncrona.

La solución SDS de la plataforma de Hiper-Convergencia debe estar esté integrada en el kernel del hipervisor.

La solución permitirá la posibilidad de crecer hasta 64 nodos en un único *cluster* de Hiper-Convergencia (no por unión de diferentes *clusters*).

La capa SDS no deberá depender de una Storage / Controller Virtual Machine en cada nodo para la gestión del almacenamiento de la solución.

Se dispondrá de un único interfaz de administración de las capas de SDS e hipervisor, desde donde poder realizar todas y cada una de las tareas necesarias (básicas y avanzadas) para la administración diaria de la solución de hiper-convergencia.

Existirán APIs disponibles para integración con PowerShell.

2.2. Elementos de respaldo

2.2.1. Descripción general

Se pretende dotar la infraestructura con determinados elementos de respaldo en una segunda ubicación geográfica a modo de contingencia, de forma que ante la eventual caída del CPD principal en caso de desastre, sea posible continuar prestando servicio desde esta segunda ubicación (CPD de respaldo).

Estos elementos de respaldo se describen en los siguientes apartados:

2.2.2. Nodo de cómputo

Como nodo de cómputo de respaldo se deberá suministrar un servidor adicional independiente que será instalado en una ubicación geográfica distinta y deberá integrarse en el *clúster* de virtualización principal, el cual deberá presentar características y capacidad suficiente para contener un mínimo de 25 máquinas virtuales con los servicios principales.

De este modo, en caso de desastre en la ubicación geográfica de los nodos principales que hicieran inviable la prestación del servicio desde los mismos, se dispondrá de este nodo de contingencia con características suficientes para prestar un servicio básico con los elementos principales necesarios para tal fin.

Para describir las características técnicas mínimas que el servidor deberá contener, se expone como ejemplo el siguiente modelo basado en un servidor PowerEdge R740XD2. El servidor deberá tener características equivalentes de igual o superior capacidad a las siguientes:

- 2 procesadores Intel Xeon Gold 5218R, 2,1 GHz, 20 núc./40 subpr., 10,4 GT/s, caché 27,5 MB, Turbo, HT (125 W)
- 768 Gb de RAM, tipo DDR4-2666, 3200 MT/s, bloque doble
- 24 discos NLSAS de 4 TB a 12 Gb/s, 7200 RPM, disco duro 512n conectable en caliente de 3,5, proporcionando una capacidad neta aprox. de unos 73TiB.
- 1 Configuración de chasis 0, 24 HDD de 3,5, PERC único, para tarjeta vertical de configuración 1 o 4
- 1 Tarjeta vertical de configuración 4, Butterfly - 1 de altura completa y 4 de perfil bajo, 2 CPU, R740XD2
- 1 Tarjeta SD redundante habilitada

- 2 Tarjetas micro-SDHC/SDXC de 64 GB
- 1 Lector de tarjetas de diferentes tipos e IDSDM
- 1 Tarjeta de controlador PERC H730P
- 1 CPU térmico estándar para chasis de 3,5
- 2 fuentes de alimentación redundantes conectables en caliente (1 + 1) de 1100 W
- 2 cables de alimentación 10 A, 2 m (6,5 pies), C13 a C14, estilo PDU
- 1 Intel® X710 10GbE, de cuatro puertos, BASE-T, adaptador, PCIe, perfil bajo
- 1 LOM integrada
- 1 Guías estáticas PEC para montaje en rack.

De igual modo, para que este servidor pueda cumplir su cometido, se deberá proveer el licenciamiento del software necesario para su prestación del servicio de virtualización, el cual debe ser 100% compatible e integrado con el del clúster principal. Por lo tanto, se proveerá una licencia tipo VMware vSphere 7 Essentials Plus Kit para 3 hosts (máx. 2 CPU por host, 32 núcleos/CPU), con 3 años de licencia y subscripción, o en todo caso equivalente, entendiendo por equivalencia la completa operatividad, prestaciones, experiencia de usuario de la plataforma principal e integración con la misma.

Toda la solución de cómputo, esto es, los nodos primarios y el nodo de respaldo, deberán ser del mismo fabricante a fin de garantizar un único punto de contacto con el objeto de minimizar los tiempos de resolución de problemas por parte del soporte técnico.

2.2.3. Orquestador failover/failback

La sincronización y transiciones de la prestación del servicio entre la plataforma principal y este nodo de respaldo (esto es, *failover* y *failback*) deberá estar orquestada por un elemento software adicional, el cual proporcione la funcionalidad de automatizar la gestión del Disaster Recovery para al menos 25 máquinas virtuales de modo que permita minimizar el tiempo sin prestar servicio en caso de un desastre.

Dicho elemento debe permitir una gestión definida por políticas, con una orquestación automatizada y que permita el testeo no disruptivo de los planes de recuperación. Debe ser capaz de automatizar no solo el *failover* sino también el *failback*.

Por último, la configuración y administración de dicho elemento deberá estar completamente integrada en la solución global, permitiendo realizar las tareas que correspondan desde una única interfaz común.

Se propone como ejemplo el producto de la suite VMware *Site Recovery Manager*, si bien se podrá suministrar cualquier otro software equivalente y funcionalmente igual o superior a éste en los aspectos mencionados.

2.2.4. Elemento de almacenamiento

Se deberá suministrar adicionalmente un elemento de almacenamiento que complemente la solución global, con el objeto de que el servicio NAS que actualmente ofrecen los Servicios Informáticos de la UAH sea servido desde dicho elemento y no directamente desde el entorno hiper-convergente, descargando al mismo de este cometido, a efectos de eficiencia en la relación coste-prestaciones.

Dicho elemento deberá ser completamente compatible y equivalente al que actualmente disponen los Servicios Informáticos de la UAH (esto es, una cabina SAN del fabricante Dell EMC, modelo Unity 380XT), con el objeto de configurar ambas en modo "espejo" replicando el contenido entre ambos y garantizando de este modo la integridad de los datos aun en caso de desastre en la ubicación de cualquiera de los dos.

El elemento de almacenamiento suministrado deberá cumplir las siguientes especificaciones:

2.2.4.1. Características generales

- Elementos hardware completamente redundados sin puntos únicos de fallo, incluyendo: doble fuente de alimentación en todos los elementos, tolerancia a cortes de corriente (de duración indefinida) sin pérdida de operaciones de escritura.
- La arquitectura propuesta debe ser unificada, es decir, debe proporcionar las funcionalidades de SAN, NAS y vVOLs en un único sistema, sin necesidad de elementos Hardware/Software adicionales aparte de los proporcionados en las controladoras del sistema.
- La solución propuesta debe tener 2 controladoras de almacenamiento actuando como unidad de alta disponibilidad. Ambas controladoras deben ser activas para todos los servicios ofrecidos, y no se aceptarán modelos basados en arquitecturas activo/pasivo desde el punto de vista de las controladoras de almacenamiento.
- Alta Disponibilidad local con 99,999% de "UpTime" certificado.
- No serán admitidas soluciones basadas en servidores y sistemas operativos de propósito general.
- Cachés espejadas para la aceleración de las operaciones de escritura y de lectura basada en memoria DIMM (no basada en discos) con tamaño mínimo de 48GB.
- Se requieren Conexiones SAS 12G multi-camino al backend de disco totalmente redundantes por procesadora.
- Proporcionará alta disponibilidad total a los datos almacenados y servidos desde el sistema de almacenamiento; contará con protección adicional tanto física como lógica (por ejemplo, "Vault Disk Cache Area") de manera que se produzca la salvaguarda correcta de los datos en caso de caída total de todos los circuitos eléctricos, que asegure la consistencia incluso ante caídas de tensión de varios días. Es indispensable la garantía de cinco nueves (99.999%) de disponibilidad del sistema por parte del fabricante.
- Proporcionará una gran escalabilidad y flexibilidad del almacenamiento permitiendo mezclar en el mismo sistema integrado (y en la misma bandeja de discos) tanto unidades NL-SAS 7200 rpm, como discos SAS 15Krpm, 10Krpm y discos Flash SSD (eMLC y TLC)
- Deberá permitir crecer la caché del sistema de almacenamiento, tanto para lectura como para escritura, hasta al menos 6.000 GB en cada cabina con el uso de tecnología SSD (eMLC). Esta caché se podrá asignar y desasignar dinámicamente y sin parada del servicio.
- Funcionalidad de discos Hot Spare globales.

- Los *pools* ALL FLASH creados en la máquina no requerirán de un disco *hotspare* dedicado, el espacio de reconstrucción se distribuirá entre los discos existentes. Permitiendo que no exista ningún disco en espera (*hotspare*) o que todos los discos participen en la reconstrucción y rendimiento de la máquina.
- Posibilidad de inserción de discos y bandejas en caliente, con soporte de balanceo automático de los datos en los volúmenes/*pools* de disco ampliados.
- Deberá permitir que ante la detección de un fallo o un posible futuro fallo (Preemptive HotSpare) en un disco, éste sea reemplazado proactivamente por el más equivalente al que presenta el problema.
- Posibilidad de Spin Down (parada física de discos rotacionales basada en políticas) en los discos.
- Deberá disponer de una arquitectura que impida que el fallo individual de un disco afecte al resto de discos en la misma bandeja.
- La caída de una controladora no supondrá ninguna disrupción en protocolos de bloques ni de ficheros, siempre que los protocolos de ficheros lo permitan.
- La Cabina a suministrar permitirá crecer en capacidad de proceso (modelo superior) de manera *in place* y *online*, sin necesidad de migración de datos.
- Se debe proporcionar un mecanismo, nativo e integrado en el software de la cabina de almacenamiento, de importación de datos de LUNs desde otros sistemas de cabinas similares y terceros, con el fin de facilitar cualquier migración o consolidación.
- Se debe poder hacer una instalación basada únicamente en software (Virtual Storage Appliance) de una solución de almacenamiento compatible con la suministrada, usable con Vmware ESXi, y con las siguientes funcionalidades:
    - Solución basada en software (Software Defined Storage) unificada con funcionalidades SAN y NAS.
    - Administrable desde vCenter.
    - Protección local mediante *snapshots*.
    - Replicación de datos hacia otras instancias de la solución de almacenamiento, tanto virtuales como basados en *appliances* físicos.
    - Optimización del uso de almacenamiento mediante *Tiering*.
    - Administración de la plataforma desde el mismo interfaz que las instancias físicas.
    - Soporte de funcionalidad de VMware vVols.
    - Soporte de VMware VAAI para SAN y NAS.
    - Soporte de VMware VASA.

2.2.4.2. Configuración

- La cabina debe tener una capacidad neta de al menos 81,5 TiB*. No se tendrán en cuenta tecnologías de compresión o deduplicación en el cómputo de la capacidad neta de la cabina.

  (*) 1 TiB = 2^{40} bytes = 1.099.511.627.776 bytes (base 2)

- Al menos un 8% de la capacidad será de tecnología Flash
- Al menos un 12% de la capacidad será tecnología SAS.

2.2.4.3. Rendimiento

- La cabina deberá ser capaz de servir hasta 12.000 IOs con un tamaño de bloque de 8k y un 40% de lectura.

2.2.4.4. Facilidad de uso

- Debe permitir una administración basada en entorno WEB. Todas las funcionalidades del sistema deberán poder ser gestionadas desde una única herramienta. Permitirá la administración desde el mismo entorno que la cabina actual de los Servicios Informáticos de la UAH.
- La cabina deberá descubrir las máquinas virtuales conectadas y asociarlas topológicamente con el servidor físico donde residen y con su almacenamiento asignado sin necesidad de agentes.
- Debe ofrecer la posibilidad de monitorización de su funcionamiento mostrando los valores oportunos de manera instantánea e histórica.
- Adicionalmente la cabina a suministrar permitirá, como licencia incluida, consultar toda la información de configuración, rendimiento y analíticas de uso desde un portal público en la nube, accesible mediante HTML5, bajo la infraestructura del fabricante. Esta funcionalidad debe dar acceso a información de rendimiento y capacidad acerca de almacenamiento y hosts, así como analíticas en tiempo real acerca de dichos datos con analíticas predictivas. No se debe requerir de ningún tipo de recurso adicional local (computacional o de almacenamiento) para su puesta en marcha, y debe almacenar al menos 3 años de datos históricos. Debe asimismo permitir un análisis sencillo de anomalías de rendimiento y capacidad.

2.2.4.5. Calidad de servicio

- Deberá disponer de una herramienta de gestión de la calidad de servicio a los servidores (QoS) a través de la cual se puedan priorizar, de manera dinámica, las IOPS o los MB de LUNS o filesystems respecto a otros.
    - La gestión de esta calidad de servicio debe realizarse de manera dinámica y a través de la misma consola de gestión, permitiendo aprovechar al máximo los recursos del sistema y eliminando así la necesidad de reservar de manera prefijada recursos del mismo.

- Deberá permitir actuar de forma automática o manual sobre los volúmenes en los que se pueda encontrar la necesidad de mejorar / reducir su calidad de servicio, permitiendo para los mismos una reubicación dinámica en un diferente tipo de disco o protección RAID, sin influir en el normal funcionamiento de las aplicaciones.

2.2.4.6. Crecimiento

- El crecimiento deberá ser modular, sin requerir interrupción en el servicio.
- Debe permitir que de manera dinámica se amplíen los volúmenes de datos (LUNs) con distribución automática de los datos sobre el espacio añadido.
- Los modelos híbridos deben permitir el crecimiento en discos con diferentes tecnologías, entre ellas, Flash SSD eMLC, TLC, SAS y NL-SAS.
- Los modelos híbridos permitirán *autotiering* con tres tipos de disco diferentes: SSD, SAS, SAS_NL. La caché no se contemplará como parte del *tiering*.
- Debe permitir la ampliación de los módulos de *Front-End*. Pudiendo elegir diferentes configuraciones de puertos como FC 4Gbps, FC 8Gbps, FC 16Gbps GbE, 10GbE, empleando tarjetas de expansión que permitan distintos tipos de interfaces físicos (cobre, ópticos…) de manera que el sistema disponga incluso de capacidad para la ampliación a tecnologías futuras sin necesidad de cambiar la controladora completa.
- Se debe poder hacer crecer la solución con discos en formatos de 3.5” y 2.5”, incluyendo una opción de bandeja de alta densidad para el formato de 2.5”, en la cual se puedan alojar 80 discos de 2.5” en un máximo de 3 *Rack Units*.
- La cabina permitirá crear volúmenes de 256TB NAS en un solo volumen y en un solo *pool*.
- La cabina permitirá compartir almacenamiento del mismo pool entre SAN y NAS recuperando el espacio ahorrado de SAN/NAS para ser ofrecido a SAN/NAS. No siendo válida la creación de distintos *pools* para diferentes propósitos.

2.2.4.7. Conectividad avanzada

- Deberá ser accesible por más de un canal en alta disponibilidad y ofrecer funciones de balanceo de carga.
- Como medida de seguridad permitirá la activación en entornos NAS de la funcionalidad IP *reflecting*. Esta funcionalidad permite el reenvío de paquetes a través de las interfaces que generaron la petición.
- La plataforma de almacenamiento en su gestión NAS permitirá la creación de dos interfaces de red con la misma IP en la misma controladora, permitiendo el acceso de diferentes *tenants* en la misma controladora.
- La cabina proveerá de componentes necesarios para que la caída de un puerto de red no suponga disrupción. Estos componentes no estarán basados en *switches* externos.

2.2.4.8. Funcionalidades de Protección de Datos

- La cabina debe ofrecer la capacidad de réplica síncrona y asíncrona tanto para la funcionalidad de SAN como para la funcionalidad de NAS, de manera unificada y desde el mismo interfaz.
- La réplica debe poder realizarse en las topologías de 1:1, 1:N y N:1.
- La cabina debe ofrecer la capacidad de realización de *snapshots* o copias Point in Time tanto para recursos de bloque como de fichero. La tecnología de *snapshots* no debe implementar *copy-on-write*.
- La creación de *snapshots* debe ser posible tanto manualmente, como mediante la aplicación de un Schedule automático.
- Se debe incorporar el concepto de Grupos de Consistencia.
- Se debe poder hacer al menos 256 *snapshots* por cada elemento.
- Se debe soportar *snapshots* jerárquicos de hasta 10 niveles.
- Todos los *snapshots* deben ser usables en modalidad lectura/escritura.
- Se deben poder aplicar políticas de Quality of Service a los *snapshots*, que no tienen por qué coincidir con la política de Quality of Service de la LUN origen.
- Cualquier *snapshot* debe poder ser refrescado desde cualquier otro.
- Se debe incluir la capacidad de replicación de *snapshots* a otra cabina similar, pudiendo especificar diferentes políticas de retención de estos entre los almacenados en origen y destino. Asimismo, se podrá especificar como destino de la réplica de *snapshots* un almacenamiento compatible con S3 para retención de largo plazo.
- El sistema deberá incluir un mecanismo para el control de la protección local y remota de datos (*snapshots* y réplica) por niveles de servicio. Este mecanismo deberá integrarse con los aplicativos para la obtención automatizada de instantáneas locales o réplicas remotas, Oracle, SQL, Exchange, VMware, etc. Gestión de hasta 20 copias concurrentes.

2.2.4.9. Gestión

- La plataforma en su conjunto podrá ser gestionada desde una única herramienta gráfica. No necesitará de elementos (java) para poder ser administrada. HTML5 requerido.
- Se dispondrá también de un interfaz de tipo CLI (línea de comandos) que permita la realización de tareas de mantenimiento / realización de scripts desde los clientes del sistema de almacenamiento y otros sistemas con conectividad al mismo.
- La plataforma de almacenamiento incluirá las librerías y API REST necesarias para el desarrollo de herramientas software de administración personalizadas.
- El acceso a la plataforma de administración se realizará empleando elementos seguros (HTTPS, SSL…).
- No se requerirán elementos externos al sistema de almacenamiento para servir las herramientas de administración (por ejemplo, servidores o SSOO de propósito general).

- El sistema incluirá herramientas gráficas de monitorización y generación de informes de uso y consumo del almacenamiento y de rendimiento. Estas herramientas deberán ofrecer de forma gráfica toda la información y posibilitar la exportación de estos datos en formatos estándar, Excel, etc.
- Incluirá una licencia que permita el envío de información de configuración y rendimiento a una nube pública externa en la que los usuarios administradores podrán consultar el estado de las diferentes cabinas de almacenamiento desde una interface HTML5 en una nube pública. Así como analíticas avanzadas del entorno.

2.2.4.10. Gestión de incidencias

- El sistema se integrará con herramientas que permitan su gestión remota, proactiva y reactiva tanto por el soporte de los sistemas como por los administradores del sistema. Deberá posibilitar la generación interna y externa de alertas SMTP o SNMP.
- No se requerirá ningún componente externo para la gestión del punto anterior.

2.2.4.11. Específicas Pool SAN

- Capacidad de servir LUNs a través de conectividad FC, iSCSI a nivel de bloque de manera nativa a través de puertos dedicados a ello en el sistema de almacenamiento, no siendo válido la emulación de dichas LUNs sobre un *filesystem* ni la conversión de protocolos a través de software *switches* o conversores.
- Flexibilidad de configuración del nivel de protección RAID (RAID 1,5, 6) controlado a nivel HARDWARE por la propia cabina de almacenamiento.
- Debe permitir la posibilidad de aprovisionar virtualmente más espacio en la LUN SAN del físicamente asignado (Virtual Provisioning).
- Deberá permitir la creación de *pools* con diferentes tecnologías de discos.
- Tendrá la capacidad de almacenar los datos en diferentes tecnologías de disco y/o niveles de protección RAID de manera que se permita alinear el valor de los datos y su actividad con el tipo de disco. El propio sistema deberá estar dotado de la inteligencia necesaria para mover, sin disrupción del servicio, dicha información tanto a nivel de volumen completo como de un subconjunto del mismo (Sub-LUN), de una manera completamente automatizada y optimizada.
- Los *snapshots* de la plataforma permitirán ser origen de réplica y tener características de QoS.

2.2.4.12. Específicas de ficheros

- La plataforma de almacenamiento tendrá la capacidad de exportar protocolos de ficheros sobre los mismos *pools* sobre los que se exportan bloques. De tal manera que las eficiencias aplicadas en ambos mundos puedan ser aprovechadas globalmente.
- La plataforma de almacenamiento deberá ser capaz de crear *filesystems* que puedan ser exportados por los siguientes protocolos: NFSv3, NFSv4, NFSv4.1; CIFS SMB 2, SMB 3 y SMB 3.1.1; FTP y SFTP; FC, e iSCSI.

- Los *filesystems* deberán crecer hasta 256TB.
- Los *filesystems* reclamarán el espacio no utilizado de manera periódica al pool, este espacio podrá ser utilizado para cualquier funcionalidad de la cabina.
- Los *filesystems* formarán parte de la política de *autotiering* permitiendo que los bloques se puedan reasignar de manera automática y desatendida. Permitirán además el cambio de políticas de prioridades online.
- La plataforma permitirá configurar contenedores de servicios de ficheros (NAS servers) que permitan configurar sus propios servicios asociados (interfaces de red, protocolos compartidos, servicios de directorio, backup, seguridad…).
- La infraestructura permitirá la réplica síncrona NAS con solamente 2 puertos FC
- Se podrá realizar backup de la infraestructura NAS mediante protocolo NDMP v1-v4 tanto en modalidad 3-Way como en modalidad 2-Way
- La funcionalidad NAS debe incorporar la capacidad de realizar *tiering* a nivel de fichero a dispositivos de Cloud pública (compatibles con S3 y Microsoft Azure) o privada, automatizando mediante el uso de políticas el movimiento de ficheros sin necesidad de intervención manual.

2.2.4.13. Específicas de virtualización

- Estará integrada con las diferentes API de VMware para almacenamiento: VAAI y VASA. Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File.
- Incluirá herramientas de administración desde hipervisores (HYPER-V, VMware) que permitan provisión administración y clonado de la plataforma de almacenamiento desde el interfaz del hipervisor.
- Incluirá soporte VMware Site Recovery Manager (SRM), permitiendo administrar *failover* y *failback*.
- Incluirá soporte para OpenStack Cinder Driver, que permita provisión y administración de los volúmenes de bloques en entornos *openstack*.
- Incluirá soporte para OpenStack Manila, que permitirá administrar *filesystems* compartidos en entornos *openstack*.
- Permitirá configurar Servidores NAS como *tenants* o grupos independientes en la cabina, de tal manera que dos servidores NAS con contenido diferente puedan exportar la información por la misma IP en diferentes VLANS.

2.2.4.14. Protocolos soportados (detalle)

- Access-based Enumeration (ABE) para protocolo SMB.
- Address Resolution Protocol (ARP) para protocolos de bloque: iSCSI, Fibre Channel (FCP SCSI-3)
- Soporte para Controller based Data at Rest Encryption (D@RE), con claves autogestionadas.

- DFS Distributed File System (Microsoft) tanto como Leaf node o Standalone Root Server.
- Direct Host Attach para Fibre Channel e iSCSI.
- Dynamic Access Control (DAC) con claims support
- Fail-Safe Networking (FSN)
- Internet Control Message Protocol (ICMP)
- Kerberos Authentication Key Management Interoperability Protocol (KMIP), con gestor de claves externo compatible con D@RE.
- LDAP (Lightweight Directory Access Protocol)
- LDAP SSL Link Aggregation para File (IEEE 802.3ad) Lock Manager (NLM) v1, v2, v3, y v4.
- Soporte para IPv4 e IPv6 tanto para puertos de Management y Servicio, como para Servidores NAS Multiprotocolo para clientes UNIX y SMB (Microsoft, Apple, Samba).
- Network Data Management Protocol (NDMP) v1-v4 tanto 3-Way como 2-Way.
- Network Information Service (NIS) Client Network Status Monitor (NSM) v1
- Network Time Protocol (NTP) client
- NFS v3/v4 Secure Support NT LAN Manager (NTLM) Portmapper v2
- REST API
- Compatibilidad con Restriction of Hazardous Substances (RoHS)
- RSVD v1 for Microsoft Hyper-V
- Simple Home Directory access para protocolo SMB
- Cliente Simple Mail Transfer Protocol (SMTP) compatible con SMI-S v 1.6.0.
- Simple Network Management Protocol v2c y v3 (SNMP)
- Virtual LAN (IEEE 802.1q)

2.2.4.15. Específicas de seguridad

- La solución debe estar validada para su uso con FIPS 140-2.
- La plataforma permitirá ser cifrada con controladoras SAS dedicadas de tal manera que no afecten al rendimiento.

2.2.4.16. Específicas de licencias

- La plataforma incluirá un solo paquete de licencias básicas que permitirán utilizar todas las características de la maquina sin necesidad de adquirir licencias adicionales.
- La cabina de almacenamiento incluirá todas las licencias de la cabina actuales y futuras durante el tiempo de mantenimiento.

2.2.5. Elemento de sincronización del almacenamiento

La solución basada en dos cabinas (la actual en los Servicios Informáticos de la UAH y la que se suministrará) permitirá la replicación de los sistemas de ficheros tanto de forma síncrona como asíncrona. La solución debe permitir una gestión automática de la creación, gestión de ciclo de vida y borrado de los *snapshots* (instantáneas temporales de la información que se almacena en un determinado momento) sobre la cabina de destino (réplica) ajustándose de forma automática a los periodos de retención que sean definidos por la Universidad.

Se suministrarán los elementos software necesarios para este cometido.

3. PRESTACIONES A REALIZAR

Las prestaciones a realizar para conseguir el objeto de este contrato son las siguientes:

- El suministro, instalación y configuración del equipamiento cuyas características técnicas se especifican en el apartado anterior.
- El soporte técnico y mantenimiento que otorga el fabricante para el sistema durante el periodo de al menos cuatro años, ampliado en su caso por el adjudicatario.
- La configuración y migración completa de datos de SAN alojados en la infraestructura actual de producción de los Servicios Informáticos de la UAH a la nueva infraestructura adquirida con arreglo a lo especificado en el apartado anterior. Para este cometido se deberá considerar como requisito prioritario la continuidad del servicio, garantizando la no interrupción siempre que sea posible, o bien la minimización de los periodos de corte cuando no exista alternativa.
- La configuración de los mecanismos de respaldo basados en los elementos especificados en el apartado anterior. De este modo, se deberá configurar:
    - La automatización de la gestión del *Disaster Recovery* para las máquinas virtuales que decida la Universidad (con un máximo de 25), basada en una gestión del *failover* y el *failback* entre los nodos hiper-convergentes y el nodo de respaldo, definida por políticas, con una orquestación automatizada y que permita el testeo no disruptivo de los planes de recuperación.
    - La replicación de los sistemas de ficheros entre la cabina de almacenamiento actual de la Universidad y el nuevo elemento de almacenamiento suministrado, de forma síncrona y asíncrona, de forma que permita una gestión automática de la creación, gestión de ciclo de vida y borrado de los *snapshots* sobre el elemento de réplica ajustándose de forma automática a los periodos de retención que sean especificados por la Universidad.

4. TRANSFERENCIA TECNOLÓGICA

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar en todo momento a las personas designadas por la UAH a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

5. PREVENCIÓN DE RIESGOS LABORALES Y COORDINACIÓN DE ACTIVIDADES EMPRESARIALES

Tanto el adjudicatario como las empresas subcontratadas o trabajadores autónomos contratados por éste cumplirán en el desarrollo de sus funciones con los requisitos legales que marca la Ley 31/1995 de Prevención de Riesgos Laborales y con el R.D 171/2004, de coordinación de actividades empresariales, en cada caso.

La empresa adjudicataria informará con suficiente antelación al Servicio de Prevención de la Universidad (servicio.prevencion@uah.es) cada vez que subcontrate trabajos a realizar en la propia Universidad, con otra empresa o trabajador autónomo, indicando la forma de coordinación preventiva establecida entre ellos.

El adjudicatario cumplirá asimismo con el procedimiento de coordinación de actividades empresariales vigente en la UAH en todo aquello que le sea aplicable.

En caso de que un trabajador de la empresa adjudicataria sufra un accidente de trabajo mientras desempeña los servicios contratados por la UAH, la empresa adjudicataria informará asimismo al Servicio de Prevención de la Universidad a la mayor brevedad posible.

Fdo.: el Director de los Servicios Informáticos