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

# SUMINISTRO DE INFRAESTRUCTURA DE BACKUP PARA LA UNIVERSIDAD DE ALCALÁ

## PLIEGO DE PRESCRIPCIONES TÉCNICAS

Universidad de Alcalá

# 1. OBJETO DEL CONTRATO

El objeto del contrato es el suministro de un repositorio de copias de seguridad (backup) para la UAH.

# 2. INTRODUCCIÓN

En este apartado se detallan los requisitos mínimos obligatorios de las actuaciones y suministros objeto del presente procedimiento de contratación. Al presentar la oferta, el licitador debe ajustarse a la terminología utilizada en este apartado.

Los requisitos detallados en este apartado no pretenden ser una relación exhaustiva de las características técnicas de los elementos demandados en el presente pliego. Éste solo recoge las características necesarias de los elementos objeto del Procedimiento de Contratación. Las ofertas de los licitadores deberán proporcionar la especificación técnica completa de dichos elementos, ya que la propuesta debe constituir una solución integral, que incluya los elementos necesarios para el cumplimiento de todos los requisitos y especificaciones técnicas descritos a lo largo del presente Pliego de Prescripciones Técnicas.

El contratista debe garantizar la integración lógica entre todos los componentes (hardware y software). Con el objeto de garantizar el correcto funcionamiento de la solución en su conjunto, la UAH se reserva el derecho a solicitar al contratista una batería de pruebas del equipamiento ofertado, y una propuesta de documentación asociada que contemple, al menos, el detalle de estas y resultados obtenidos.

Como objetivos principales de este procedimiento caben destacar, con carácter general:

- La implantación de soluciones de backup a disco basadas en appliances específicos de backup (PBBA – Purpose Built Backup Appliance) con deduplicación online, por bloque variable e integrados con la solución de protección de datos para proporcionar deduplicación en origen, en un único pool de deduplicación global, integrados con el software de backup a través de protocolo OST (DDBoost).
- La reducción de los tiempos de backup actuales, así como la aceleración de los tiempos de recuperación ante pérdida de datos o desastres.
- La disponibilidad de múltiples copias de seguridad en diferentes localizaciones para garantizar la recuperación ante desastres.
- La necesidad de replicar los volúmenes de backup por líneas IP entre los dos CPD´s de que dispone la UAH.
- La reducción del tiempo de gestión de las operativas de backup actuales.
- La posibilidad de dotar a la solución de mecanismos de movimiento de datos (larga retención y/o DR) hacia soluciones de cinta y/o de cloud (Privada/Hibrida o pública), mediante protocolos eficientes como S3.
- El repositorio global debe ser capaz a futuro de integrarse con las aplicaciones Enterprise que posea la UAH como son Oracle y PostgreSQL, proporcionando a estas aplicaciones funcionalidades de backup a disco con deduplicación en origen, integradas con los distintos gestores de Backup De Datos.

- La solución debe incorporar algoritmos de deduplicación eficientes integrados con el software de backup.
- La solución debe incorporar la posibilidad de múltiples protocolos de accesos como son SMB, NFS, VTL y NDMP. Permitiendo independientemente del protocolo de acceso al *appliance* por cualquiera de los protocolos exigidos una deduplicación global para todo el entorno.

## 3. REQUISITOS DEL HARDWARE

Se pretende dotar a la UAH de una solución de repositorio avanzado de Protección de Datos para cada uno de los 2 CPD existentes. Se deberá suministrar para cada uno de los 2 CPDs, un *appliance* específico de backup a disco, de iguales características. Los componentes ofertados deberán estar integrados entre sí a nivel lógico (gestión, administración y operación). La solución ofertada deberá permitir realizar copias locales en cada uno de los CPDs que serán almacenadas en los *appliances* ofertados en el presente procedimiento.

Así mismo la solución ofertada permitirá replicar o clonar copias individuales de backup entre los 2 CPDs, enviando únicamente información deduplicada por la red.

El sistema deberá ser una solución unificada de hardware y software de propósito específico de backup. No se admitirán soluciones basadas en servidor o cabinas de almacenamiento de propósito general.

Los *appliances* específicos de protección, deben poder replicarse y permitir la migración desde los dispositivos actuales que posee la UAH.

Cada uno de los *appliances* tendrá una capacidad neta de almacenaje para backups de al menos 92Tb. Se entiende como tamaño neto el tamaño del disco una vez formateado, con el grupo de paridad ya establecido, y sin contar la posible reducción de espacio que se obtenga con el sistema de deduplicación.

Los *appliances* ofertados deberán estar licenciados para utilizar toda la capacidad de disco ofertada.

Los *appliances* ofertados deberán estar integrados con el software de backup ofertado. No obstante, los *appliances* deberán ser compatibles y poder ser utilizados con otros softwares de backup y archivado del mercado, al menos: Veritas NetBackup, Dell Avamar, Veeam, Data Protector, Dell NetWorker y Commvault.

Los *appliances* deberán utilizar tecnología de reducción de datos basada en deduplicación y compresión. La deduplicación deberá realizarse in-line y deberá ser global a toda la información protegida en el *appliance*.

Se debe garantizar una ratio de deduplicación más compresión global mínimo superior a 40:1 (97% de reducción).

La tecnología de deduplicación de los *appliances* deberá ser de segmentación variable automática, con tamaños de bloque desde 4KB, para asegurar una mayor reducción de los datos almacenados.

Deberá poder realizar preprocesado de los segmentos de datos (deduplicación en origen).

Aunque el ofertante deberá ofertar la capacidad y prestaciones que estime necesarias para cada CPD, cómo mínimo deberá ofertar:

- Una capacidad de 92 TB netos/usables por sistema
- Este sistema deberá ser escalable como mínimo hasta 172 TB netos y ser capaz de dar un rendimiento de 24 TB / hora. Se deberá aportar hoja de especificaciones del fabricante.
- Los sistemas deben tener mecanismos de desborde hacia Cloud (Privada o pública) sin necesidad de gateways externos y manteniendo el mismo algoritmo y ratio de deduplicación.
- Licenciamiento de desborde hacia cloud de hasta 144 TB usables.
- Los sistemas deben tener redundados aquellos elementos HW que sean susceptibles de fallo (fuentes de alimentación, ventiladores).
- Deben tener como mínimo memoria NVRAM 16 GB
- Deben poseer como mínimo 192 GB de memoria RAM
- Deben de disponer como mínimo de conectividad 10 GbE base T (4 puertos) / FC 16Gbits y 10GbE SFP+.
- Los sistemas deben poder ser capaces de absorber hasta 270 streams de datos (Backup, restores y réplicas) de forma paralelizada.

Los *appliances* deben tener la funcionalidad y consideración especial con los entornos de BBDD de Oracle, permitiendo integrar funcionalidades avanzadas de Oracle, optimizando de forma lógica los datos recibidos y permitiendo altas tasas de deduplicación de las mismas.

Los *appliances* ofertados deberán poder replicar los datos entre sí, de forma deduplicada, asegurando que por la red sólo se envían los bloques únicos.

La replicación de los backups deberá poder realizarse de forma paralela al proceso de backup (inline) para acortar los tiempos de recuperación ante desastres.

Todos los procesos internos de gestión de la información de los *appliances* se deben realizar en paralelo a cualquier otro proceso de backup, restore y/o réplica, sin perjuicio de la función principal de estos repositorios de protección orientados al backup que es la restauración del dato y su protección.

Los *appliances* ofertados deberán ser capaces de incluir como mínimo los protocolos de acceso CIFS, NFS, DD Boost, VTL y NDMP. Estos protocolos podrán ser ofrecidos de forma simultánea y la deduplicación deberá ser global independientemente del protocolo utilizado para almacenar los datos

Los *appliances* ofertados tendrán la posibilidad de añadir posteriormente los protocolos VTL (Virtual Tape Library) y NDMP a través de FC. Como mínimo deberán poder emular 128 drives por cada VTL.

Los *appliances* ofertados tendrán la capacidad de integrarse con software Enterprise de BBDD como Oracle, DB2 y SQL Server, entre otros, sin necesidad de la intervención de software de backup.

Los *appliances* ofertados tendrán la posibilidad de gestionar cuotas soft y hard, para evitar y gestionar el crecimiento indiscriminado de volumen protegido por aplicación o servicio de protección.

Los *appliances* ofertados deben replicarse a través de líneas de comunicación IP, evitando repercutir en un coste de líneas FC para realizar las réplicas deduplicadas entre ellas.

Los *appliances* de protección deben tener la capacidad de cifrado de la información que reside en ellos, sin merma en la deduplicación global ofrecida por el sistema.

Los *appliances* de protección deben ser capaces de ofrecer tenants lógicos para las distintas aplicaciones, encapsulando de forma lógica la información y evitando el acceso no seguro a los mismos.

# 4. REQUISITOS DEL SOFTWARE

Se proveerá la solución de software de backup a implantar para la realización de copias de seguridad en los *appliances* descritos en el apartado anterior. Los requisitos mínimos obligatorios son los siguientes:

- A fin de garantizar la plena integración entre el software y el hardware que componen la solución, ambos componentes deberán pertenecer a un mismo fabricante global de soluciones de backup.
- Se dotará de licencia de software de backup corporativa basada en la capacidad de procesamiento de los sistemas de origen, siendo ésta de un mínimo de 45 sockets.
- A fin de mantener compatibilidad de datos históricos y su capacidad de recuperación de los mismos, la nueva solución debe tener compatibilidad total con toda la información y datos históricos mantenidos en el sistema de backup actual de los SSII de la UAH, sin necesidad de adaptación, migración o conversión de los mismos, permitiendo su recuperación inmediata sobre la nueva solución a implantar.
- Debe permitir la realización de backup de los entornos virtuales VMware, permitiendo granularidad de restauración a nivel de fichero tanto para máquinas virtuales Windows como Linux.
- Debe integrarse con la funcionalidad de CBT (Changed Block Tracking) de VMware tanto en backup como en restore.
- Para realizar el backup de entornos VMware debe utilizar proxies virtuales (no se aceptarán soluciones que requieran de un proxy físico) y el software deberá tener un sistema de balanceo de carga para repartir la carga de backups de las máquinas virtuales entre los diferentes proxies virtuales disponibles.
- Debe permitir la clonación de backups de máquinas virtuales VMware desde dispositivos de disco a dispositivos de cinta para larga retención, manteniendo siempre el software el catálogo de la información.
- Debe permitir la autoprotección de las nuevas máquinas virtuales VMware que se creen, basado en políticas automáticas a nivel de folder, etiqueta o servidor ESX, sin necesidad de intervención por parte del administrador.

- Debe permitir gestionar los backups y los restores de VMware desde la interfaz Webclient de vSphere, permitiendo a los administradores de VMware administrar sus propios backups.
- Debe permitir la restauración de backups de máquinas Windows físicas convirtiéndolas en máquinas virtuales (P2V) en entornos VMware.
- Debe soportarse y estar licenciada la posibilidad de hacer backup NDMP de sistemas NAS.
- Debe permitirse el backup a disco de aplicaciones Enterprise (Oracle – RMAN) de forma desatendida a través de agente desplegado sobre las máquinas virtuales/físicas sin coste para el cliente, pudiendo el software de backup de una forma automatizada llevarse esos datos hacia otro dispositivo (cinta) para larga retención.
- Debe ser una solución de protección de datos Enterprise, permitiendo la protección del entorno heterogéneo de la UAH, en concreto debe permitir la protección a través de Módulos de aplicación para realizar backup en caliente de al menos las siguientes aplicaciones: SQL Server, Oracle, MySQL, Active Directory.
- El software de backup debe ser capaz de orquestar la replicación de los contenidos entre los dos *appliances* ofertados y tener en un único catálogo tanto los backups de cada CPD como sus distintas réplicas o clonados, de forma que en caso de desastre en un CPD o no accesibilidad al *appliance* ubicado en él, el software sea capaz de restaurar los backups del *appliance* situado en el centro de respaldo, sin necesidad de recatalogar los contenidos.
- Debe ser capaz de realizar backups a disco basados en bloques para servidores Windows, de forma que cada vez que se haga backup sólo se haga de los bloques que han cambiado, evitando escanear todo el filesystem o crear nuevos índices en cada ocasión. Así mismo la restauración en estos casos deberá ser granular a nivel de fichero.
- Debe poder realizar backup en caliente consistente de Microsoft SQL Server con la posibilidad de restaurar granularmente. Así mismo, el administrador de SQL deberá poder realizar backups ad hoc desde la consola de gestión SQL Server Management Studio, sin necesidad de realizar la petición desde la consola de administración del software de backup.
- Debe poder realizar backup en caliente consistente de Oracle 19c y 21c con la posibilidad de restaurar granularmente. Así mismo, el administrador de Oracle podrá realizar backups ad hoc desde la utilidad de Oracle RMAN sin necesidad de lanzarlo desde el software de backup, y éste deberá catalogar los backups que se hayan lanzado desde RMAN, para que el administrador del sistema tenga un control total sobre todos los backups realizados.
- El producto deberá contener un elemento de preprocesado de deduplicación, a fin de trasmitir menos información y acelerar el rendimiento de la actual solución de backup a disco desplegada. Debe garantizar asimismo la réplica consistente entre los *appliance* de backup ofertados en este procedimiento, al objeto de posibilitar restauraciones de cualquier CPD sin intervención manual, todo ello gestionado desde la consola de gestión del software de backup ofertado.
- Deberá tener mecanismos de deduplicación en origen, no solamente para los datos de Sistema Operativo sino para los aplicativos que la UAH tiene en producción, y deben

estar integrados con los *appliances* de backup ofertados en este mismo procedimiento, de forma que el software de backup utilice el mismo algoritmo de deduplicación que los *appliance* ofertados.

- La solución deberá incorporar mecanismos automáticos de backup y restauración del repositorio de metadatos que permitan realizar operaciones Disaster/Recovery del propio servicio de backup. La continuidad del servicio de backup debe ser válida en entornos de servidores físicos y/o virtuales.

## 5. REQUISITOS DE LOS SERVICIOS PROFESIONALES

Se ofertarán los servicios profesionales adecuados para la instalación del entorno, los cuales deben incluir tanto la instalación física de los equipos como la instalación, configuración y parametrización del software que compone la solución, principalmente:

- Despliegue y configuración inicial de la infraestructura (*appliances*).
- Configuración de los *appliances* a nivel lógico en el entorno de backup.
- Redefinición y reconfiguración de las políticas de backup para su adaptación al nuevo entorno, con arreglo a los requerimientos de la UAH.
- Migración de los datos contenidos en el entorno actual de backup de la UAH a los nuevos dispositivos.
- Pruebas de validación del entorno, las cuales se deberán realizar conjuntamente con el personal designado al respecto en la UAH.

Durante el transcurso del despliegue, se realizarán reuniones de seguimiento periódicamente con el objeto de supervisar y garantizar la adecuada evolución del mismo, detectando y permitiendo corregir las posibles desviaciones respecto a la planificación.

Además, se ofertarán los servicios profesionales necesarios para la documentación y transferencia de conocimiento del entorno desplegado a los Servicios Informáticos de la UAH, a fin de que la gestión del mismo pueda ser llevada a cabo de forma autónoma de manera interna en la organización. El tiempo dedicado a la transferencia de conocimiento deberá ser de al menos 15 horas hábiles repartidas en tres jornadas de 5 horas cada una, las cuáles se organizarán con arreglo a un plan detallado a elaborar conjuntamente entre la UAH y el prestatario, pudiendo abarcar tanto las personalizaciones específicas del despliegue como aspectos más generales sobre el hardware o el software desplegados, a modo de curso de formación general sobre la tecnología implantada.

Los servicios profesionales deberán ser realizados por personal técnico cualificado y certificado en la solución por el fabricante.

## 6. MANTENIMIENTO

El mantenimiento correspondiente al hardware suministrado será de 48 meses (4 años) a contar desde la fecha de puesta en servicio de la infraestructura suministrada.

Este mantenimiento deberá comprender como mínimo el soporte que otorga el fabricante relativo a:

- Mantenimiento evolutivo y preventivo, mediante el suministro de las actualizaciones de firmware del producto (bien versiones evolutivas o bien parcheado preventivo) que sean desarrolladas y publicadas durante el tiempo de vigencia del contrato.
- Mantenimiento correctivo, mediante el soporte técnico necesario para solventar cuantas incidencias o averías técnicas se produzcan relacionadas con el producto durante dicho periodo, tanto en el software como en el hardware que lo compone. Quedarán por tanto incluidos todos los trabajos y las piezas (discos, fuentes de alimentación, entre otros) que puedan ser necesarios para restablecer por completo el estado del sistema.

A su vez, los trabajos de instalación y configuración del producto, la migración de los datos, y en general las actuaciones de cualquier tipo sobre el entorno quedarán garantizadas ante cualquier problema derivado de estas tareas durante un periodo de 12 meses (1 año) a contar desde la puesta en servicio de la cabina.

## 7. PRESTACIONES A REALIZAR

En resumen, las prestaciones a realizar en este contrato son las siguientes:

- El suministro, instalación y configuración del equipamiento, cuyas características técnicas se especifican en los apartados correspondientes.
- La prestación de los servicios profesionales que procedan en cada caso:
    - La configuración y parametrización del entorno para que cumpla el cometido especificado en los correspondientes apartados, así como su documentación y transferencia de conocimiento a la UAH.
- El soporte técnico y mantenimiento que otorga el fabricante para todos los elementos del entorno durante el periodo de cuatro años.

## 8. TRANSFERENCIA TECNOLÓGICA

Durante la ejecución de los trabajos objeto del contrato, el contratista 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.

## 9. PREVENCIÓN DE RIESGOS LABORALES Y COORDINACIÓN DE ACTIVIDADES EMPRESARIALES

Tanto el contratista 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.

El contratista 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 contratista 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 del contratista sufra un accidente de trabajo mientras desempeña los servicios contratados por la UAH, el contratista informará asimismo al Servicio de Prevención de la Universidad a la mayor brevedad posible.

[Firmado electrónicamente]

por: Manuel Cabrera Silva

Cargo: Director de los Servicios Informáticos

Firmado digitalmente por CABRERA SILVA MANUEL - DNI 08966521V
'Fecha: 2022.06.30 17:15:21 +02'00