PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DEL SUMINISTRO DE UNA PLATAFORMA DE BACKUP CONVERGENTE, A ADJUDICAR POR PROCEDIMIENTO ABIERTO SUJETO A REGULACIÓN ARMONIZADA.
REF: TSA000067639

El objeto de este pliego es el suministro, incluidos los servicios de soporte técnico y mantenimiento, así como la instalación, configuración y puesta en marcha, de una plataforma de backup convergente, que deberá reunir las características técnicas y elementos mínimos detallados en los apartados siguientes.

Las condiciones a continuación especificadas serán de aplicación a la totalidad del suministro y su cumplimiento será supervisado y evaluado por personal técnico del Grupo Tragsa.

Situación actual

A día de hoy se están utilizando 2 sistemas de backup distintos en los CPDs corporativos de la Organización.

1.1. CPDs Maldonado y Julián Camarillo 6B

En estos 2 CPDs se utiliza una misma herramienta de backup. Esta solución está desplegada sobre las siguientes máquinas para su correcto funcionamiento:

- 2 servidores virtuales (uno en cada CPD) funcionando en modo activo/pasivo que se encargan de la gestión centralizada del sistema.
- 4 servidores físicos (2 en cada CPD) que realizan las tareas de movimiento de datos entre las máquinas de las que se realiza backup y los sistemas de almacenamiento de destino.
- 7 servidores virtuales (3 en el CPD de Maldonado y 4 en el de JC6B) que actúan como proxies del sistema de backup para la realización de las copias de máquinas virtuales.
- 2 cabinas (1 en cada CPD) donde se guardan todas las copias de seguridad. Cada una de estas cabinas proporciona una capacidad útil de 355TB.

Adicionalmente la solución requiere que se despliegue al menos un agente (pueden ser varios en función de la(s) aplicación(es) a proteger) en cada uno de los equipos no virtuales (o virtuales si se hace copia de alguna aplicación que se ejecute en ellos) de los que se vaya a hacer backup. Así, a día de hoy se han desplegado un total de 205 agentes.

La solución está dimensionada para realizar backups de aproximadamente 238TB (85TB en Maldonado y 153TB en JC6B) y permitir una retención máxima de las copias de seguridad de 60 días.

1.2. CPD Valentín Beato 6

En este CPD se utiliza una herramienta de backup distinta a las anteriores. Esta solución está desplegada sobre las siguientes máquinas para su correcto funcionamiento:

- 1 servidor que realizar las funciones de gestión centralizada del sistema, así como del movimiento de datos entre las máquinas de las que se realiza backup y los sistemas de almacenamiento de destino.
- 1 librería de cintas magnéticas con 2 unidades de lectura/escritura y 25 slots para cintas.

Adicionalmente la solución requiere que se despliegue al menos un agente (pueden ser varios en función de la(s) aplicación(es) a proteger) en cada uno de los equipos de los que se vaya a hacer backup. Así, a día de hoy se han desplegado un total de 18 agentes.

La solución está dimensionada para realizar backups de aproximadamente 20TB y permitir una retención máxima de las copias de seguridad de 60 días.

1.3. Caracterización de datos

En la siguiente tabla se caracterizan los distintos tipos de datos de los que se realiza backup en cada uno de los CPDs:

CPD	Nombre	Tipo	#VMs	Tamaño (TiB)	Ratio Crecimiento Anual (%)	Ratio Cambio Diario (%)
Maldonado	BD	Datos estructurados	N/A	9	10	5
Maldonado	Imágenes	Datos no deduplicables	N/A	10	1	1.7
Maldonado	NAS	Datos no estructurados	N/A	33	1	1
Maldonado	VMs	VMs genéricas	300	33	10	1
JC6B	Imágenes	Datos no deduplicables	N/A	40	1	1.7
JC6B	NAS	Datos no estructurados	N/A	50	1	1
JC6B	VMs	VMs genéricas	600	63	10	1
VB6	BD	Datos estructurados	N/A	5	10	5
VB6	Imágenes	Datos no deduplicables	N/A	5	1	1
VB6	NAS	Datos no estructurados	600	10	1	1

Situación objetivo

El gran número de elementos que componen la solución actual comporta un alto grado de complejidad tanto en el funcionamiento de la misma como en su gestión y operación. Adicionalmente, desde hace algún tiempo se está produciendo un elevado número de incidencias, que está requiriendo un extra de dedicación por parte del personal del Grupo Tragsa y que está influyendo negativamente en la fiabilidad del sistema.

La situación de destino busca sustituir la plataforma actual por una homogénea, de tipo convergente tanto en computación como en almacenamiento, basada en hardware generalista de tipo x86 y compuesta por un número de nodos, organizados en uno o más clústeres, suficiente para proporcionar el servicio descrito.

Dicha plataforma deberá integrar el hardware y el software necesario reduciendo la complejidad de gestión y ampliando los tiempos máximos de retención de las copias de seguridad.

Para ello, se sustituirán todos los servidores físicos y virtuales de todos los CPDs y la librería de cintas magnéticas de Valentín Beato. Se mantendrán las 2 cabinas de Maldonado y JC6B enviándose a ellas las copias más antiguas.

La nueva plataforma no deberá requerir de gestión separada del hardware, S.O. y software de backup, sino que se deberá realizar de forma unificada desde una única consola para toda la plataforma.

El sistema se dimensionará para poder hacer backup de aproximadamente 300 TB de datos aumentando la retención de las copias de seguridad hasta un mínimo de 5 meses.

Así mismo, el diseño de la solución deberá contemplar que siempre exista una 2ª copia de los datos en un CPD distinto al de origen.

Características obligatorias de la plataforma a suministrar

Las prestaciones y requisitos que se enumeran a continuación son obligatorios (todos ellos y de forma simultánea) **y su no cumplimiento implica la exclusión de la licitación.** *Los licitadores deberán ofertar todos y cada uno de los elementos solicitados, sin excepción, para ser tenidas en cuenta en el proceso de valoración.*

- Plataforma de backup de tipo convergente tanto en computación como en almacenamiento, basado en hardware generalista de tipo x86 y compuesto por nodos, típicamente (aunque no necesariamente) en bloques de 2RU con 4 nodos cada bloque.
- La plataforma debe contar con el almacenamiento propio suficiente para almacenar todas las copias de seguridad que tengan una antigüedad, como mínimo, inferior a 2 semanas.
- La solución debe desplegar al menos un clúster en el CPD de Maldonado y otro en el de JC6B.
- El sistema de backup debe estar totalmente autocontenido, es decir, no se aceptarán soluciones que estén conformadas por diferentes componentes tipo catálogo, gestor de medios, proxies, BBDD de búsqueda, BBDD de deduplicación, etc., ya sea de forma externa (VMs o máquinas físicas), como de forma interna en "appliance" de backup (con virtualizador interno y los diferentes componentes virtualizados)
- Sistema con escalabilidad ilimitada, sin puntos únicos de fallo y basado en el concepto de "webscale" y "masterless", donde todas las tareas y trabajos sean balanceados por todo el hardware del sistema de forma automática.
- El sistema de backup debe de tener, en su arquitectura, capacidades de almacenamiento de alto rendimiento para servir metadatos y ficheros con necesidades de latencia de acceso menor y garantizar unos niveles de RTO óptimos.
- La ampliación del sistema debe realizarse de forma automática, sin necesidad de creación de nuevos componentes de backup (VMs, componentes, etc.) o reasignación manual de tareas, recursos, espacio, etc.; debe ser suficiente con ampliar el clúster scale-out y el propio sistema hará el rebalanceo de tareas y datos sobre el nuevo hardware.
- Un clúster debe permitir mezcla de tipo de nodos, generaciones y capacidades.
- El sistema debe auto recuperarse y recomponerse ante fallos hardware
- El sistema debe ser 100% API Restful sin dependencias de terceros de tal manera que sea compatible con cualquier tipo de dispositivo.
- La solución de backup deberá ser accesible y gestionada de manera unificada y sencilla por parte de los administradores del entorno.
- El interfaz de administración debe ser único para todos los tipos de backup y residir en el propio sistema de backup. Debe estar basado en HTML5.
- El sistema debe disponer de un elemento de gestión global, que monitorice los diferentes sistemas de backup individuales.
- Se deberán poder definir usuarios locales, Roles de administración personalizados e integrar la seguridad con Directorio Activo y directorios LDAP.

- El sistema de backup debe tener un motor de búsqueda de objetos de backup y de ficheros de tipo google, predictivo, y con tiempo de respuesta cercano a 0, independientemente de donde se encuentre el backup del objeto en cuestión (backup local o archivo remoto).
- El sistema de backup debe incluir un sistema de reporting avanzado, basado en HTML, configurable y planificable.
- La solución dispondrá de un sistema de creación de alertas sobre múltiples categorías, que permita envío de correos y generación de acciones asociadas.
- Las políticas de protección incluirán la posibilidad de replicar copias, aplicando distintos períodos de retención, de forma deduplicada, comprimida y encriptada.
- El backup debe ser en formato primer "full" e incremental para siempre para todo tipo de objeto. No se aceptarán "full" backups periódicos más incrementales/sintéticos.
- El sistema de backup debe soportar sistemas de archivo basado en NFS y en protocolo de almacenamiento de objetos S3, tanto en nube pública como privada. Y en concreto deberá poder exportar, vía NFS, las copias más antiguas a las cabinas del Grupo Tragsa hasta una capacidad total mínima de 650TB.
- El sistema debe proporcionar inmutabilidad para los backups, de tal manera que no puedan ser borrados de forma maliciosa o afectados por un ramsonware/malware. Es decir, los backups no serán depositados en repositorios CIFS/NFS/FS genéricos.
- Se deberá poder realizar encriptación del contenido, utilizándose mecanismos internos de gestión de claves, con posibilidad de utilizar alguna solución externa de gestión de las mismas.
- La solución deberá tener, dentro de sus características y funcionalidades, la posibilidad de realizar trabajos de respaldo y restauración de manera consistente, granular y de poder aplicar diferentes niveles de retención de las políticas establecidas y también la posibilidad de realizar réplicas de datos entre diferentes sedes y/o localizaciones y archivado a otras arquitecturas.
- El sistema de backup deberá tener mecanismos de eficiencia en el almacenamiento, como son la deduplicación y compresión, para el ahorro y optimización de las capacidades.
- La solución de backup permitirá la protección de entornos Windows y Linux.
- La solución de backup permitirá la protección de VMs de VMware, MS HyperV y Nutanix AHV, así como recuperación granular de ficheros en las mismas.
- La solución de backup permitirá realizar backup en caliente de MS SQL Server, con posibilidad de recuperación completa y PIT. Se debe soportar AAG y Failover cluster.
- La solución de backup permitirá realizar backup en caliente de MS Exchange, así como un sistema de recuperación granular de objetos de MS Exchange para un mínimo de 15.000 buzones.

- La solución de backup permitirá realizar copias en caliente de MS Sharepoint, así como un sistema de recuperación granular de objetos de MS Sharepoint para un mínimo de 75TB de almacenamiento de esta aplicación.
- La solución de backup deberá incluir la posibilidad de realizar backups consistentes de bases de datos Oracle, así como un sistema de recuperación granular a nivel de base de datos.
- El sistema debe realizar backup de sistema de ficheros, tanto de servidores como de servicios y cabinas NAS.
- El sistema debe ser capaz de mostrar imágenes de los backups de VM y BBDD Oracle y SQL Server, en modo lectura/escritura de forma casi inmediata (RTO casi 0), desde el propio sistema de backup, en disco SSD, sin afectar a la propia imagen del backup o a otros existentes.
- EL sistema de backup debe autodescubrir nuevas instancias de BBDD en el servidor, y asignarles los SLAs de backup correspondientes, y nuevas BBDD individuales dentro de las instancias, asignándoles el SLA correspondiente.

Servicios de instalación, configuración y puesta en marcha

Las ofertas deben incluir los siguientes servicios mínimos: Instalación, configuración y puesta en marcha. En concreto:

- Transporte a los CPDs de Grupo Tragsa.
- Diseño de la solución. Diseño de alto nivel con componentes hardware y software, así como necesidades de comunicaciones para la integración con el resto de los componentes de producción.
- Instalación física de los elementos en los CPD de Grupo Tragsa y del cableado intra-rack que conecte entre sí los diferentes elementos.
- Retirada y reciclaje de los embalajes.
- Instalación y configuración de la nueva solución. De acuerdo al diseño aprobado y las mejores prácticas para cada componente.
- Configuración de las copias de seguridad de un subconjunto de los sistemas de los que se realizan dichas copias con el sistema actual, incluyendo al menos un sistema de cada tipo (VMs, MS Exchange, MS SharePoint, MS SQL Server, Oracle DB, NAS).
- Pruebas de funcionalidad. Según se acuerde para garantizar la correcta implantación.
- Elaboración y prueba de los procedimientos de contingencia que sean aplicables a los distintos elementos en respuesta a errores y averías.
- Formación oficial o a medida para la correcta operación de la solución

- Los servicios de instalación, configuración, puesta en marcha y mantenimiento deberán ser realizados obligatoriamente por técnico/s certificado/s por el fabricante.

Condiciones que deberá reunir el servicio de soporte técnico y mantenimiento durante el período de garantía:

Activación de toda la solución en el servicio de soporte técnico del fabricante, facilitando al Grupo Tragsa el procedimiento a seguir para la apertura y seguimiento de incidencias hasta su cierre.

- Duración: Cinco años.
- Acceso al personal de apoyo durante 365x7x24, prioridad en las llamadas y en el manejo de casos y con reemplazo de piezas in situ NBD.
- Atención telefónica y soporte Web con tiempo de respuesta no superior a 4 horas.
- Soporte técnico in situ para reemplazo de piezas si fuera necesario.
- Atención telefónica de incidencias y consultas por parte de técnicos cualificados para ayudar a la resolución de:
  - Problemas de producto: Dudas de funcionalidad, actualización de versiones, información de errores conocidos, etc.
  - Problemas de sistema: Asesoramiento en parametrización, comprobación de logs, sugerencias de administración, etc.
- Suministro y operativa de las actualizaciones de software/firmware a versiones posteriores que surjan durante el período de vigencia del servicio de mantenimiento.
- Acceso al portal de clientes con la información más reciente sobre productos, documentación, parches y preguntas más frecuentes.
- Todas las actuaciones que se realicen al amparo del contrato de soporte y mantenimiento por parte del adjudicatario serán realizadas por técnicos debidamente certificados por el fabricante de los productos.

Los referidos requisitos deben entenderse como mínimos pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. Las propuestas que ofrezcan características o prestaciones inferiores a las exigidas no serán tomadas en consideración en el presente procedimiento.

No se admite la presentación de variantes.

Madrid, 18 de julio de 2019

Grupo Tragsa (Grupo SEPI) · Sede Social: Maldonado, 58 · 28006 Madrid · Tel.: 91 396 34 00 · www.tragsa.es