

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA  
LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA  
CONTRATACIÓN DE SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y  
PUESTA EN MARCHA DE UNA PLATAFORMA DE BACKUP  
CENTRALIZADA.**

**ENMARcado EN EL “PLAN DE RECUPERACIÓN,  
TRANSFORMACIÓN Y  
RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA - NEXT  
GENERATION EU”**

**Componente 5, Inversión 1 del PRTR**

**A-5.2.3. “Plataforma de backup centralizado”**

**Donostia / San Sebastián, diciembre de 2024**

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN,  
MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DE SUMINISTRO,  
INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA PLATAFORMA DE  
BACKUP CENTRALIZADA.**

**ENMARcado EN EL “PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y  
RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA - NEXT  
GENERATION EU”**

**Contenido**

|    |                                                                               |   |
|----|-------------------------------------------------------------------------------|---|
| 1  | Antecedentes.....                                                             | 1 |
| 2  | Objeto del contrato .....                                                     | 2 |
| 3  | Características técnicas del appliance de Backup .....                        | 2 |
| 4  | Características técnicas del software de Backup .....                         | 6 |
| 5  | Planificación .....                                                           | 7 |
| 6  | Plazo de garantía.....                                                        | 8 |
| 7  | Documentación a presentar por la empresa contratista .....                    | 8 |
| 8  | Etiquetado verde y etiquetado digital .....                                   | 8 |
| 9  | Principio de no causar perjuicio significativo al medio ambiente (DNSH) ..... | 8 |
| 10 | Obligaciones de comunicación .....                                            | 9 |

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN,  
MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DE SUMINISTRO,  
INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA PLATAFORMA DE  
BACKUP CENTRALIZADA.**

**ENMARCADO EN EL “PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y  
RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA - NEXT  
GENERATION EU”**

**Componente 5, Inversión 1 del PRTR**

**A-5.2.3. “Plataforma de backup centralizado”**

**1 Antecedentes**

La evolución de las TIC ha traído consigo un gran incremento de sistemas y aplicaciones (máquinas virtuales, bases de datos SQL, sistemas de archivos, equipos finales, etc.) cada uno con su propio método de *backup* (copia de seguridad), y con el paso del tiempo, se ha observado que la necesidad de capacidad de almacenamiento de *backup* se está incrementando notablemente. Además, la falta de un protocolo unificado ha creado confusión sobre qué sistema utilizar para cada tipo de *backup*, aumentando el riesgo de errores operativos. Esta situación se complica aún más con la necesidad de cumplir con diferentes regulaciones de protección de datos, lo que requiere una gestión de *backup* meticulosa y bien documentada.

En una empresa como Aguas del Añarbe, la seguridad y la integridad de los datos son de suma importancia y por tanto en los últimos años se ha sido testigo de un aumento significativo en los ataques de ransomware, que no solo amenazan la continuidad del negocio, sino que también ponen en riesgo la disponibilidad y la integridad de los datos críticos de nuestra organización.

La adquisición de un sistema de *backup* centralizado con la capacidad de ejecutar copias inmutables es esencial para nuestra estrategia de ciberseguridad. Las copias inmutables, que no pueden ser alteradas ni eliminadas una vez creadas, son una defensa crítica contra el *ransomware*. Esto se debe a que, incluso si nuestros sistemas son comprometidos, los datos respaldados permanecerán intactos y accesibles, lo que nos permitirá restaurar rápidamente la operatividad sin ceder ante las demandas de los atacantes.

Además, un sistema de *backup* centralizado mejorará la eficiencia operativa al simplificar la gestión de los respaldos y reducir la complejidad asociada con los sistemas de *backup* distribuidos. Esto no solo optimizará los recursos, sino que también reducirá el riesgo de errores humanos, que es una causa común de pérdida de datos.

Con esta actuación, se pretende dotar a las distintas Áreas de Aguas del Añarbe de un sistema centralizado, cómodo, seguro y fiable, sobre el que poder realizar las copias de

seguridad de la información más crítica existente. La idea es mejorar la capacidad de retención, mejorar los tiempos de RPO y RTO y dotar a ese repositorio central de la capacidad de marcar copias de los datos como inmutables para protegerlas de ataques tipo ransomware.

## **2 Objeto del contrato**

El presente contrato tiene por objeto:

- Por un lado, el suministro, instalación, configuración y puesta en marcha de un *Appliance* de *backup* en disco con deduplicación con destino al centro de proceso de datos de AGASA situado en las oficinas centrales de Paseo de Errotaburu (Donostia).

Este equipo deberá cubrir las necesidades de copia para garantizar el respaldo de archivos, bases de datos, máquinas virtuales y cualquier otra información considerada de carácter importante para AGASA, unificando sistemas y aumentando las prestaciones de velocidad y almacenamiento actuales.

- Por otro lado, la adquisición de las licencias de software de respaldo de datos con capacidad de gestionar las copias de seguridad en entornos virtuales, físicos y en la nube.

## **3 Características técnicas del appliance de Backup**

Se deberá suministrar un *Appliance* específico de *backup* a disco y las licencias de software que este pueda necesitar para operar. El licitador deberá presentar una propuesta con equipos de última generación. La solución aportada por el licitador, deberá ser una única solución integral, es decir, hardware y software deberán estar integrados entre sí a nivel lógico (gestión, administración y operación). Deberá estar basada en un *Appliance* de propósito específico para copias de seguridad y restauración de la información.

No se aceptarán soluciones que requieran de hardware adicional al *Appliance*, bien sean servidores de medios (*media servers*) o discos de almacenamiento externo al *Appliance*.

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 puesto que tales sistemas no están optimizados en rendimiento.

La solución ofertada no deberá tener costes ocultos que supongan adquisición de hardware o software adicional por parte de AGASA y en el caso de que se pusieran de manifiesto durante la ejecución del contrato, o bien una vez implantada la solución, serán de cuenta del adjudicatario.

La solución ofertada deberá integrarse con el entorno productivo de AGASA basado en la plataforma hiperconvergente HPE Simplivity.

Características del hardware y requisitos mínimos:

- El sistema propuesto debe ofrecer una controladora base con las siguientes características:
  - Mínimo de dos (2) CPU AMD con 8 “cores” cada uno
  - Mínimo de 512GB RAM, de tipo DDR4-3200
  - Mínimo de cuatro (4) puertos de 1/10GBase-T Ethernet
  - Mínimo de dos (2) discos dedicados para contener el sistema operativo
- Debe admitir el etiquetado de VLAN. Los puertos IP que se ofrecen del mismo tipo también admitirán agregaciones de puertos (*port bonding*).
- El sistema propuesto debe ofrecer un mínimo de 80 TB de espacio local bruto (RAW), distribuido en discos de 8 TB. Debe poder escalar hasta como mínimo 250 TB de espacio local bruto (RAW).
- El sistema propuesto debe ofrecer un mínimo de 50 TB espacio neto local, siendo escalable también hasta al menos 200 TB de capacidad neta local, y unos 400 TB adicionales de capacidad neta usando almacenamiento en la nube como AWS, Azure o sobre un almacenamiento de objetos S3-compatible.
- Se considera la capacidad neta local como: el resultado de restar la capacidad bruta local del sistema (RAW) el espacio necesario para la implementación de la protección de la información (grupos de RAID, discos de *hot spare*) sin aplicar ninguna técnica de ahorro en disco como deduplicación, y/o compresión. Tampoco se considerará por el cálculo de espacio local la capacidad externa que pueda consumirse en la nube pública o privada.
- Debe tener una única capa de almacenamiento local activa para operar con los datos. No se permitirán configuraciones con movimiento interno o archivado de la información en una capa secundaria de disco dentro del almacenamiento local del mismo repositorio.
- Debe poder ofrecer un rendimiento sostenido de escritura de al menos 5 TB/hr.
- Debe incorporar todas las licencias necesarias para implementar las funcionalidades de deduplicación/compresión y réplica optimizada (permitiendo la transmisión de bloques únicos no duplicados).

El detalle de **las características relacionadas con eficiencias en el almacenamiento** que deben satisfacerse para cada PPBA sigue a continuación:

- El sistema debe integrar un motor de deduplicación obligatoriamente *in-line*, haciendo la optimización de espacio antes de la escritura en los discos físicos. No se permitirán dispositivos que utilicen de duplicación post proceso.
- El algoritmo de la deduplicación debe poder trabajar obligatoriamente tamaños de bloque variable sobre los datos de *backup*, para reconocer un mayor número de patrones repetidos y garantizar la máxima eficiencia en el envío y almacenamiento de datos en el mismo repositorio.
- Adicionalmente a la deduplicación, debe integrar obligatoriamente la compresión *in-line* de los datos, es decir, antes de la escritura sobre los discos físicos. No se permitirán dispositivos que utilicen compresión postproceso.

El detalle de las **características relacionadas con la protección de la información y seguridad** que deben satisfacerse para cada PPBA sigue a continuación:

- El sistema propuesto debe proteger los datos mediante un RAID 6 hardware, que vendrá configurado de fábrica y no requerirá manipulaciones adicionales durante la fase de instalación. De tener que escalar el tamaño, se incorporarían discos en grupos RAID 6 adicionales.
- Adicionalmente, debe incorporar como mínimo un (1) disco en rol de *hot spare* por cada grupo de RAID.
- Debe disponer de mecanismos de revisión y verificación continuos durante la ingesta de la información, y periódicamente, sobre los datos ya almacenados para asegurar la consistencia de la información.
- Debe soportar la funcionalidad de encriptación *data-at-rest*, que cumplan la validación FIPS140-2. El cifrado de los datos debe realizarse después del procedimiento de deduplicación, pudiéndose ejecutar sobre la totalidad del repositorio, así como sobre volúmenes parciales.
- Adicionalmente, también deberá soportar la funcionalidad de *Secure Erase*, a fin de garantizar que no se pueda recuperar datos de forma no autorizada. Es necesario que cumpla NIST SP800-88, realizando un mínimo de siete (7) sobre escrituras aleatorias.
- Debe incluir mecanismos de seguridad para garantizar la protección frente a ataques de ransomware y otros programas malignos (*malware*).
  - Autorización dual: el sistema requerirá de un sistema de autorización dual mediante un usuario específico de seguridad para validar la ejecución o no de las operaciones críticas sobre el sistema (modificar y/o borrar un volumen/todo el almacenamiento, cambio en la fecha/hora, desactivación de la funcionalidad de autorización dual).
  - Inmutabilidad: el sistema podrá configurar un período de inmutabilidad como mínimo a nivel de volumen.

El detalle de las **características relacionadas con los tipos de acceso al dato** que deben satisfacerse para cada PPBA sigue a continuación:

- El sistema propuesto debe soportar acceso *VTL FC*, *VTL ISCSI*, *NFS exports* y *SMB shares* como repositorio de *backup*, con acceso concurrente para cada uno de ellos.
- Deberá poder emular, como mínimo, los formatos de cintas LTO-5, LTO-6 y LTO-7.
- Debe tener la capacidad de configurar al menos una combinación de 64 bibliotecas de cintas y objetivos NAS junto con 100.000 o más ranuras de cartuchos en un único dispositivo.
- Debe tener inteligencia para entender tanto la deduplicación basada en origen como en destino y debe integrarse con el software de *backup* en producción actual o futuro de AGASA (*CommVault*, *VeeamB&R*).
- Adicionalmente, debe estar certificado para poder trabajar con el resto de principales proveedores del mercado, *Veeam*, *Zerto*, entre otros.
- El dispositivo propuesto será capaz de ofrecer su almacenamiento de forma directa e integrada en las aplicaciones de *backup*, de forma que se optimicen las transferencias de datos y no sea necesario utilizar los modos VTL ni NAS. Se requiere integración de esta funcionalidad por el software de *backup* actualmente en producción en AGASA, como mínimo. Esta capacidad permite realizar las tareas de deduplicación en origen utilizando el mismo algoritmo que implementa el dispositivo de disco.
- Debe admitir también, mediante el motor de deduplicación nativo del sistema de almacenamiento, la recepción y/o envío de forma optimizada de datos de y/o hacia entornos de backup parejos, ubicados en otros centros de datos:
  - Aplicación de deduplicación en la transmisión desde su origen.
  - Descargando de ciclos de cómputo de los servidores de medios de la herramienta de *backup*, ya que los datos se transmiten de *Appliance* a *Appliance*. Los servidores de *backup* pasan a gestionar y monitorizar el proceso.
  - Esta funcionalidad debe ser compatible tanto para *CommVault* como *VeeamB&R*.

El detalle de las **características relacionadas con la monitorización y gestión remota** que deben satisfacerse para el *appliance* de copias de seguridad (PBBA) sigue a continuación:

- El sistema propuesto debe soportar monitorización local y en la nube, que muestre:
  - Licenciamiento.
  - Configuración detallada del hardware instalado.

- Información global y parcial sobre la capacidad actual, la eficiencia del almacenamiento por volumen de datos y la predicción automática de la capacidad futura del sistema.
- Lista de casos abiertos con soporte (sólo en la nube).
- Avisos de actualizaciones disponibles por el sistema (sólo en la nube).
- Debe ser integrable en una plataforma de monitorización basada en protocolo SNMP.
- Debe poder gestionar de forma cómoda mediante una interfase gráfica (GUI), que también tendrá la posibilidad de gestionar de forma centralizada el resto de PBBA (*appliance* de copias de seguridad) a incorporar en el entorno de AGASA.
- Complementariamente, desde el GUI del sistema propuesto deberá mostrar la información agregada del resto de sistemas de *backup* con el mismo sistema operativo o superior del entorno.
- Debe incluir de una herramienta de gestión, monitorización y reporte integrada en un procesador dedicado (ASIC) dentro de la placa base del equipo.
  - El acceso se realizará mediante un puerto 1GBase-T dedicado (OOBM, fuera de banda).
  - Proporcionará una API REST de gestión de acuerdo con la especificación Redfish DMTF.
  - Cumplimiento de: FIPS140-2, CNSA, SSL/TLS 256 bits, autenticación 2FA.
  - Soporte de alertas de componentes hardware críticos: CPU, memoria y disco.
  - Funcionalidad de actualización de firmware.

#### **4 Características técnicas del software de Backup**

El software ofertado ha de ofrecer capacidades confiables de respaldo, recuperación y replicación, asegurando la continuidad del negocio y minimizando el tiempo de inactividad en caso de desastres o pérdida de datos.

El software ha de ofrecer licencias para posibilitar el *backup* (copia de seguridad) de un mínimo de 50 máquinas virtuales. Dichas licencias tendrán una validez de cinco años.

#### **Características Principales**

1. **Protección Integral:** se han de poder proteger todos los datos, ya sea en la nube, virtuales o físicos, sin las restricciones o complejidades de las soluciones de respaldo tradicionales.
2. **Escalabilidad y Flexibilidad:** La solución debe permitir el escalado de manera confiable y ha de adaptarse a las necesidades del negocio, protegiendo todo, desde bases de datos y aplicaciones hasta datos de usuarios.

3. **Recuperación Instantánea:** ha de proveer recuperación instantánea para diferentes cargas de trabajo; máquinas virtuales, servidores físicos, NAS, bases de datos y estaciones de trabajo. Multiplataforma, VMware, Hyper-V, ...
4. **Restauración segura:** el software ha de analizar automáticamente los datos en busca de *malware* durante la restauración e identificar el punto de restauración limpio más reciente, utilizando sus propias capacidades integradas o las herramientas de detección de amenazas de terceros.
5. **Licenciamiento por instancias, no por sockets:** licencias portables y licenciamiento en base a cargas de trabajo (máquina virtual, instancia *cloud*, servidor físico, base de datos, datos no estructurados, ...)
6. **Portabilidad:** formato de respaldo diseñado para ser portátil a través de múltiples nubes, plataformas, entornos y hardware.
7. **Integración Nativa:** respaldos rápidos y de bajo impacto mediante la integración con herramientas nativas, incluyendo Microsoft VSS, Oracle RMAN, SAP Backint y Kubernetes API. Además, el software de *backup* se debe integrar con todos los protocolos del *appliance* de copias de seguridad (*ddboost* o *catalyst*) e integración con dicho *appliance* de copias de seguridad (PBBA) para permitir *backup* inmutables.
8. **Seguridad de Datos:** respaldos a prueba de ransomware con funcionalidad de bloqueo de objetos S3 y respaldos inmutables.
9. **Garantía de Recuperación:** recuperación con respaldos confiables que se prueben automáticamente para detectar ciber-amenazas y configuraciones incorrectas.
10. **Protección de Kubernetes:** que permita respaldar y recuperar aplicaciones en contenedores.
11. **Instalación:** el orquestador se ha de poder instalar “*on premise*”.
12. **Optimización:** deduplicación y compresión por “*Job*”.

## 5 Planificación

Para la realización de las referidas tareas se han estimado las siguientes fases:

- Fase 1 – Inicio De Proyecto, Análisis y Diseño.
- Fase 2– Instalación física.
- Fase 3– Configuración del entorno.
- Fase 4– Pruebas.
- Fase 5 – Documentación y cierre.
- Fase 6 – Soporte Post Arranque por parte del Licitador (15 días)

## **6 Plazo de garantía**

El plazo de garantía se establece en cinco años a contar desde la puesta en marcha de la plataforma, con la conformidad de los responsables técnicos de AGASA.

En el plazo de garantía señalado se incluirá la resolución de incidencias con respuesta en 2 horas de lunes a viernes en horario de 9:00 a 16:00, las actualizaciones y reposición de piezas averiadas y sustitución de las mismas *in-situ* el siguiente día laborable.

## **7 Documentación a presentar por la empresa contratista**

Tras la entrega del equipo en centro de proceso de datos de AGASA:

- Documentación técnica de los equipos suministrados.
- Documentación de la infraestructura y la configuración.

## **8 Etiquetado verde y etiquetado digital**

Esta actuación contribuye de manera directa a la transición ecológica. En concreto, se incluye en la etiqueta climática N° 041bis, incluida en el Anexo VI del Reglamento de Recuperación y Resiliencia, contribuyendo con un 40% a los objetivos climáticos y un 100% a los objetivos ambientales. No obstante, no contribuye de manera directa a la transición digital.

## **9 Principio de no causar perjuicio significativo al medio ambiente (DNSH)**

El contratista y los posibles subcontratistas garantizarán el respeto al principio de «no causar un perjuicio significativo» (DNSH), exigido por el REGLAMENTO (UE) 2021/241, por el que se establece el Mecanismo de Recuperación y Resiliencia y el artículo 17 del Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020 relativo al establecimiento de un marco para facilitar las inversiones sostenibles y por el que se modifica el Reglamento (UE) 2019/2088. En particular se cumplirá con la Comunicación de la Comisión Guía técnica 2021/C 58/01, sobre la aplicación del principio de «no causar un perjuicio significativo».

A estos efectos, deberán suscribir una declaración responsable, como la que figura a modo de Anexo en la Carátula de la presente licitación sobre el cumplimiento de “no causar un perjuicio significativo” (DNSH) a los 6 objetivos medioambientales en el sentido del Artículo 17 del Reglamento (UE) 2020/852.

## **10 Obligaciones de comunicación**

La entidad contratista y subcontratistas, si fuera el caso, estarán obligadas a cumplir las obligaciones de información y publicidad establecidas en el Artículo 9. Comunicación, de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

Concretamente, estarán obligados a cumplir las siguientes obligaciones:

- a) En los documentos de trabajo, así como en los informes y en cualquier tipo de soporte que se utilice en las actuaciones necesarias para el objeto del contrato, deberá exhibirse de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga "financiado por la Unión Europea - NextGenerationEU", junto al logo del PRTR y contener tanto en su encabezamiento como en su cuerpo de desarrollo la siguiente referencia «Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU».
- b) En las medidas de información y comunicación, sea cual fuere el canal de comunicación que se emplee, se deberá a hacer referencia a que la inversión está financiada por la Unión Europea a través del Mecanismo de Recuperación y Resiliencia-NextGeneration EU, instrumento financiero de la inversión C5.I1. «Materialización de actuaciones de depuración, saneamiento, eficiencia, ahorro, reutilización y seguridad de infraestructuras» del Plan de Recuperación, Transformación y Resiliencia.
- c) El órgano de contratación proporcionará durante la ejecución del contrato las indicaciones acerca del contenido preciso en cada medio y/o formato.
- d) Cuando proceda, se indicará la siguiente cláusula de exención de responsabilidad: «Financiado por la Unión Europea - NextGenerationEU. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente los del autor/a o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de las mismas».