ANEXO III

PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN Y MANTENIMIENTO DE LA SOLUCIÓN DEL SISTEMA DE COPIAS DE SEGURIDAD EN EL PARLAMENTO DE NAVARRA.

Contenido

OBJETO DEL CONTRATO

El objetivo de esta licitación es la renovación integral del sistema de copias de seguridad del Parlamento de Navarra.

Esta renovación incluye tanto la adquisición de un software de copias de seguridad (backup), como la adquisición del hardware para realizar y albergar las copias, la puesta en marcha de todo el sistema de copias, el soporte de todo el sistema, tanto del software como del hardware de copias, ambos durante 5 años y la formación sobre el manejo del software de copias.

La solución de copias de seguridad a implementar se deberá realizar sobre hardware de propósito general. El suministro de este hardware es objeto de esta licitación y se determinarán más adelante los requisitos mínimos del mismo.

SISTEMA ACTUAL

Sistema de copias

Parlamento dispone en estos momentos de un software de copias de seguridad basado en productos de ARC. Estos son ARC UDP versión 9.2 para el sistema de copias a disco y ARC Backup para el sistema de copias a cinta.

Copias en sede principal

Parlamento realiza las copias de seguridad a disco en un appliance de ARC para su primera copia a disco. Además, se realizan copias periódicas a cinta LTO 7 de todos sus sistemas de información.

Réplica de copias

Como parte del sistema de copias actual Parlamento de Navarra dispone de equipamiento de copias fuera de la sede del Parlamento. En dicho CPD se almacena una réplica completa de todas las copias a disco realizadas en la sede principal. Esta réplica está automatizada dentro de los planes de copia y se realiza cada vez que se hace una copia a disco en la sede.

Planes de copia actuales

A modo orientativo estos son los planes de copias a disco implementados en la actualidad. Estos planes deberán ser implementados en el nuevo sistema de copias como se detallará más adelante.

	Lunes	Martes	Miércoles	Jueves	Viernes	SABADO	DOMINGO	MES	HORA
Backup Maquinas físicas (agora2)	x	x	x	x	x				20:30
Backup Maquinas físicas						x			9:00
Backup Maquinas físicas								x	9:00
Réplica máquinas físicas	x	x	x	x	x	x		x	tras copia
Backup Maquinas virtuales	x	x	x	x	x				22:00
Backup Maquinas virtuales						x			8:00
Backup Maquinas virtuales								x	8:00
Réplica Máquinas virtuales	x	x	x	x	x	x		x	tras copia
Backup Maquinas virtuales con agente	x	x	x	x	x				21:00
Backup Maquinas virtuales con agente						x			7:00
Backup Maquinas virtuales con agente								x	7:00
Replica Maquinas virtuales con agente	x	x	x	x	x	x		x	tras copia
Backup Maquinas virtuales semanal						x			7:00
Backup Maquinas virtuales semanal								x	7:00
Replica máquinas virtuales linux semanal						x		x	tras copias
Backup SRVCOPIAS	x	x	x	x	x				6:00
Backup SRVCOPIAS						x			6:00
Backup SRVCOPIAS								x	6:00
Replica SRVCOPIAS	x	x	x	x	x	x		x	tras copia
Backup SRVAPLARC									6:00
BACKUP VCENTER	x	x	x	x	x				6:00
BACKUP VCENTER						x			6:00
BACKUP VCENTER								x	6:00
Replica VCENTER	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-1 Quaz e Indexador GEDE	x	x	x	x	x				1:00
GONCE-1 (PRE y PRO)						x			1:00
GONCE-1 (PRE y PRO)								x	1:00
Replica GONCE-1	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-7 PostgreSQL	x	x	x	x	x				1:30
GONCE-7 (PRE y PRO)						x			1:30
GONCE-7 (PRE y PRO)								x	1:30
Replica GONCE-7	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-4 Temporales GEDE	x	x	x	x	x				1:45
GONCE-4 (PRE y PRO)						x			1:45
GONCE-4 (PRE y PRO)								x	1:45
Replica GONCE-4	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-6 Alfresco	x	x	x	x	x				2:00
GONCE-6 (PRE y PRO)						x			2:00
GONCE-6 (PRE y PRO)								x	2:00
Replica GONCE-6	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-8 ElasticSearch	x	x	x	x	x				2:15
GONCE-8 (PRE y PRO)						x			2:15
GONCE-8 (PRE y PRO)								x	2:15
Replica GONCE-8	x	x	x	x	x	x		x	tras copia
BACKUP GONCE-2,3,5 Resto VMs	x	x	x	x	x				2:45
GONCE-2,3,5 (PRE y PRO)						x			2:45
GONCE-2,3,5 (PRE y PRO)								x	2:45
Replica GONCE-2,3,5	x	x	x	x	x	x		x	tras copia
BACKUP historico_audivisuales									1:00
srvdvd, seneca mastars.								x	1:00

Infraestructura tecnológica Parlamento

Los sistemas de los que se debe hacer copia de seguridad son la totalidad de los sistemas TIC del Parlamento de Navarra.

Infraestructura de virtualización

Estos sistemas constan de 74 máquinas virtuales alojadas en tres host ESXI versión 8.0 update 3 y orquestadas por un Vcenter en versión 8.03.

El sistema de almacenamiento utilizado para esta infraestructura es una cabina IBM Flash System 5300 y una NetApp 2820.

En la actualidad se hace copia de seguridad de todas las máquinas virtuales indicadas usando para ello un proxy de copias y los snapshot generados por Vcenter.

Además, está instalado un agente del programa de copias en algunos servidores para facilitar la restauración granular y más completa de determinados servidores.

Los servidores respaldados son servidores Windows 2019, Windows 2022 y servidores Linux con distribuciones Ubuntu, Debian, Rocky.

Se dispone de un proxy Linux para hacer restauraciones granulares de dichos servidores.

Infraestructura física

Además, se dispone de dos servidores físicos con SO Windows Server 2022 de los que también se hacen copias de seguridad. Estos servidores tienen una ocupación aproximada de 2,5 Tb. En la actualidad tienen instalado un agente del programa de copias y se hace copia de estos con dicho agente, tanto de los datos como de los sistemas operativos.

El almacenamiento de estos servidores físicos se encuentra también en las mismas cabinas mencionadas anteriormente.

Cabinas de almacenamiento

Parlamento de Navarra dispone además de otras cabinas de almacenamiento, algunas de ellas en fin de vida pero que se pueden utilizar ante una contingencia grave.

Estas cabinas son una 3PAR 8200 y una IBM 5035.

Electrónica de red y fibra

La electrónica de red de Parlamento de Navarra consta en su parte CORE con switches en alta disponibilidad de la marca EXTREME, concretamente dos equipos modelo X695-48Y con interfaces de red a 25 Gbps. Además, para la red de almacenamiento se usa electrónica de fibra de la marca DELL en alta disponibilidad, concretamente dos equipos DELL DS6610-B con ópticas a 16 Gbps.

La conexión al CPD externo se hace con un par de fibras monomodo encontrándose en el otro CPD un equipo EXTREME modelo X590-24 con velocidad a 10 Gbps, disponiendo de ópticas bidireccionales en ambos extremos lo que da una doble conexión de 10 Gbps.

ALCANCE DEL CONTRATO

La solución propuesta deberá ser de tipo llave en mano y deberá incluir:

- **Todos los elementos software necesarios para la instalación de la solución de copias de seguridad requerida, tanto en el CPD principal de Parlamento como en el CPD secundario para albergar la réplica de estas copias**. Esto deberá incluir el licenciamiento del sistema operativo de los servidores. Se deberá incluir el software de copias de seguridad y las licencias de uso del mismo para **5 años.**
- **Todos los elementos hardware necesarios para la instalación de la solución de copias de seguridad requerida, tanto en el CPD principal de Parlamento como en el CPD secundario para albergar la réplica de estas copias**. Esto serán 2 servidores con soporte y mantenimiento durante **5 años**.
- **Servicio de instalación y puesta en marcha** de todos los elementos hardware y software que se requieran a continuación en este pliego, así como la implementación de los planes de copia que se indicarán, la implementación de

las tareas de réplicas, la puesta en marcha de las medidas de control, supervisión y seguridad de las copias.

- **El servicio de mantenimiento y soporte hardware y software de la solución durante 5 años in situ**, con soporte para resolver incidencias, actualizaciones de versiones y averías de hardware.
- **La capacitación y formación** al personal técnico de Parlamento para la operación y configuración del sistema.

SUMINISTRO DE SOFTWARE Y DE LICENCIAS DE SISTEMA DE COPIAS DE SEGURIDAD

El objeto de esta licitación es el suministro de un software de copias de seguridad (backup) y de sus licencias que cubran las necesidades que se describen a continuación:

Licencias de producto de copias de seguridad para hacer copia de seguridad de 80 máquinas virtuales sin límite de la capacidad de almacenamiento de estas ni de la ocupación del backup. La capacidad de almacenamiento de los backups solo vendrá determinada por la capacidad total de los discos de los servidores de backup, para el caso de las máquinas virtuales.

Se requieren además licencias para respaldar los dos servidores físicos Windows Server 2022 con una capacidad de 3 Tb total de las copias. Las licencias requeridas serán para copia de archivos y de los sistemas operativos de los servidores, así como para poder hacer restauraciones bare metal de estos. **Estas licencias deberán incluir funcionalidades de archivado.**

Se requerirán las licencias para poder hacer análisis de riesgos en el sistema de copias y en las copias, así como de búsqueda de amenazas en las mismas.

Se requerirán licencias para recuperaciones avanzadas de directorio activo de 200 usuarios que se detallarán más adelante.

El sistema de copias de las réplicas deberá estar licenciado de la misma manera que el de copias principal, siendo necesario hacer réplica de todas las máquinas virtuales de las que se hace copia y de todos los servidores físicos y de la totalidad de su almacenamiento. La capacidad de los sistemas de réplicas vendrá por tanto únicamente determinada por la capacidad de almacenamiento total del servidor de réplicas.

Requerimientos funcionales generales del nuevo sistema de copias

El sistema de copias deberá tener los siguientes requerimientos funcionales.

- Permitir la programación de tareas de backup de toda la infraestructura de servidores detallada con anterioridad, así como la ejecución de tareas de copias bajo demanda. Las copias deberán permitir la restitución de los servidores

respaldados en caso de contingencia grave o perdida de datos. Esta recuperación podrá ser de toda una instancia de servidor completa, de su restitución bare metal en caso de equipos físicos, así como una recuperación granular de las copias almacenadas (carpetas, archivos, objetos de bases de datos, elementos del directorio activo, etc).

- El sistema deberá estar formado por soluciones hardware de propósito general y por software de propósito específico para llevar a cabo estas copias y su restauración en caso necesario. Todos los elementos suministrados deberán ser de fabricantes ampliamente reconocidos y posicionados en el sector.
- **El sistema de copias dispondrá de mecanismos de autoprotección** para, en caso de desastre total, poder recuperar el servicio de restauración de forma inmediata, simplemente accediendo a las copias realizadas con anterioridad, aunque haya indisponibilidad temporal del catálogo.
- El sistema de copias deberá poder trabajar con cualquier tipo de almacenamiento de los principales líderes de mercado, de cualquier tecnología y fabricante, garantizando de esta forma la viabilidad de la solución de cara al futuro.
- Soportará de manera integrada las copias a dispositivos como cinta/VTL de forma nativa.

Sobre los Backup

- La solución estará basada en sistema de copias a disco con el concepto de incrementales infinitas o similar. Esto significa que la solución hará una primera copia completa de los datos y las posteriores serán diferenciales, mostrando siempre para restaurar de manera gráfica y sencilla el estado completo de la copia de cada servidor actualizada.
- La solución permitirá las copias a cinta LTO. Estas copias se deberán gestionar desde la misma consola que las de disco.
- La aplicación permitirá definir planes de copias con rotación y retención de las mismas siendo esta gestión totalmente automatizada por parte del software.
- La aplicación permitirá hacer réplica de las copias a otro servidor ubicado en otro CPD. Esta réplica se podrá también programar y automatizar. Estas replicas deberán ser de tipo “air gap” garantizando la seguridad de las mismas y su aislamiento completo de la red.
- El software soportará gestión de datos para hacer backup de los sistemas de ficheros de los principales sistemas operativos, incluyendo:
    - Microsoft Windows Server.
    - Linux: Debian, CentOS, SuSE, Ubuntu, Rocky.
    - UNIX: AIX, Solaris, FreeBSD.
    - NAS.
- La solución hará copias completas de máquinas virtuales de al menos los siguientes hypervisores: VMWARE Vsphere, Microsoft HYPER-V, NUTANIX,

Proxmox VE. La solución hará copias completas de máquinas físicas con sistemas operativos Windows y linux.

- La solución hará copias de bases de datos y de todos sus objetos. En especial de estos motores de bases de datos:
    - Microsoft SQL Server.
    - Oracle.
    - MySql.
    - PostgreSQL.
- **Las copias de máquinas virtuales se podrán hacer sin agente instalado en las mismas incluido en los servidores de bases de datos, aunque se deberá poder hacer instalación del mismo en caso necesario**.
- La solución hará copias del directorio activo de Microsoft y deberá ser capaz de proteger todos los objetos de dicho directorio.
- **La solución debe ser capaz de hacer copias del Directorio Activo de Parlamento de Navarra de la instancia de Azure**.
- La solución proporcionará la capacidad de integración con *snapshots* de cabina multimarca, concretamente IBM, NetApp, HPE, EMC, Hitachi, Huawei, Pure Storage, así como con *snapshots* de almacenamiento y servicios en la nube pública (AWS, Azure).
- **La solución dispondrá de mecanismos de deduplicación** dependientes de la naturaleza de los datos y con capacidad de deduplicación tanto con bloque de tamaño fijo como con bloques de tamaño variable. Esta capacidad de deduplicación se hará en origen y no necesitará de elementos externos hardware deduplicadores. La herramienta de copias informará sobre la deduplicación general obtenida en los almacenes de copia.
- **La solución tendrá capacidad de hacer copias de seguridad de Microsoft 365 administradas y gestionadas desde la misma consola**. No es objeto de esta licitación la adquisición de licencias para este producto. Pero sí puede ser necesario hacerlo a futuro, dado que Parlamento de Navarra tiene licencias Microsoft 365.
- **El software de copia podrá usar los almacenamientos que ofrecen los principales proveedores de servicio cloud (AWS, Azure, GCP, OCI, Alibaba) para que estos sean utilizados como repositorios de backup**. Además, el fabricante del software deberá disponer de su propio servicio de almacenamiento en la nube de tipo frecuente o infrecuente garantizando inmutabilidad de las copias y sin costes ocultos a la hora de descargar información. No es objeto de esta licitación la contratación en estos momentos de este servicio, pero se podrá requerir en fases posteriores si se quiere dotar de otro nivel de seguridad mayor al sistema de copias. Esta funcionalidad deberá estar integrada en la consola de administración de la solución cuando se requiera su contratación.

- **La solución dispondrá de funcionalidades de réplica de los backups a otros repositorios, bien en la infraestructura propia de Parlamento, objeto esto de esta licitación o bien a repositorios de la nube**.

Sobre la recuperación

- El sistema de copias permitirá hacer restauraciones de los datos respaldados tanto desde las copias de disco, las réplicas de disco, desde las cintas LTO y de repositorios en la nube.
- La restauración de máquinas virtuales podrá ser de máquinas completas, de discos completos o granular tanto de carpetas, archivos, bases de datos, objetos de bases de datos, tanto de servidores Windows como de servidores Linux. Esta restauración podrá ser a la máquina actual, a una máquina virtual diferente o a un hypervisor distinto.
- La restauración granular de bases de datos será permitida mediante la instalación de agente en las mismas y sin agente en máquinas virtuales.
- La restauración de servidores físicos podrá ser a nivel de fichero, bare metal, servidor completo, y además se podrá hacer una restauración de servidor físico a máquina virtual, concretamente a los hipervisores de vSphere de VMWARE y de Microsoft Hyper-V. Esta restauración de físico a virtual también deberá ser posible a repositorios de la nube como Azure o Amazon.
- Capacidad de protección con recuperación *cross conversion,* es decir, posibilidad de recuperar un servidor virtual convirtiéndolo en el proceso del formato nativo a otro formato bajo distintos hipervisores en modalidad *on premise* (entre ellos Hyper-V a vSphere o viceversa), además de recuperación entre distintas plataformas en nube, recuperación de *on premise* a nube, y de nube a *on premise*.
- **La restauración de DA será granular en todos los objetos del mismo. También se podrá hacer restauración de Azure AD**.
- **Se podrán levantar las máquinas virtuales de manera inmediata desde las propias copias en el hypervisor de virtualización de Parlamento de Navarra, vSphere, sin necesidad de hacer restauración de los datos**. Esta funcionalidad de Live Mount o similar permitirá además de levantar la máquina de la copia hacer una restauración de la misma de manera paralela con el fin de disminuir el RTO del sistema en caso de contingencia.
- La solución tendrá la capacidad ante un desastre de replicar los datos y sincronizarlos a múltiples localizaciones con el fin de levantar la infraestructura desde estas. Esto se deberá poder hacer entre la copia “on premise” y sistemas tanto “on premise” como en la nube.
- La solución tendrá la capacidad de montar planes de recuperación automatizados para validar el estado de las copias y por tanto de tener las

máquinas levantadas en otro hypervisor para minimizar el tiempo de recuperación del sistema (RTO).

- La solución deberá disponer de planes de restauración con tareas de orquestación y recuperación de activos con propósitos de pruebas rutinarias de restauración y/o plan de recuperación y preparación.
- La solución podrá restaurar copias sin límite de tiempo, incluso no disponiendo ya de licencia activa del producto. Es decir, Parlamento de Navarra será dueña del dato y de la información almacenada, pudiendo hacer uso de ella sin límite de tiempo.

Requerimientos técnicos de la solución.

Arquitectura

El software debe ofrecer una solución única, basada en arquitectura común para los siguientes requerimientos de gestión de datos en un entorno profesional.

- **Backup y Recuperación.**
- **Archivado.**
- **Deduplicación de datos.**
- **Indexación de contenidos.**
- **Gestión de snapshots.**
- **Replicación de datos.**
- **Inmutabilidad de las copias y las réplicas.**
- **Herramientas de ciber resiliencia para garantizar la seguridad del sistema y las copias.**
- **Gestión de ciclo de vida de las copias.**
- **Gestión de informes.**
- **Seguimiento de medios**.

La solución de copias no deberá ofrecer puntos únicos de fallo. Su arquitectura deberá desligar el plano de control del plano de datos evitando que la afectación de uno de los componentes comprometa el resto de la plataforma.

La solución tendrá capacidad de montarse en alta disponibilidad.

La solución se deberá poder instalar en sistemas operativos Linux y Windows.

El software deberá proveer de una consola única y gráfica para la administración, configuración y monitorización de todas las tareas necesarias en cada uno de los entornos de copia y réplica.

El software debe disponer de priorización de trabajos para clientes específicos, tipos de agentes y cargas de trabajo.

Administración

- La solución se deberá administrar desde una única consola WEB.
- El sistema deberá ser securizado y poder ser integrado con Directorio Activo para el acceso a la consola de gestión.
- Se deberán poder crear usuarios con distintos perfiles y roles de acceso de tipo administración, operación y supervisión.
- **El acceso a la consola se podrá implementar con doble factor de autenticación (MFA).**
- **El sistema deberá ofrecer opciones de Multi-Person Authorization (MPA, 4 Eyes) para proteger el sistema ante riesgos y acciones mal intencionadas con credenciales comprometidas.**

Seguridad

El software debe tener estas capacidades integradas en la solución en cuestiones referentes a la seguridad de la solución y de las copias. Debe tener capacidad de análisis de amenazas en las copias.

- **Todas las copias que el software genere deben tener mecanismos de inmutabilidad de las mismas**, que garanticen que no pueden ser cifradas ni alteradas. Estas medidas deben ser de bloqueo del almacenamiento y de controles de acceso de los procesos y servicios que corren en los repositorios de copia, garantizando que solo el software de copia pueda escribir en los repositorios de copia.
- Estas medidas de bloqueo deberán proteger también la propia instalación del software y las configuraciones y bases de datos de la gestión del sistema de copias. Estas opciones deberán ser configurables para poder establecer distintos niveles de bloqueo.
- **La solución de copias deberá garantizar la integridad y verificación de las copias mediante procedimientos automatizados que verifiquen las copias y la restauración**.
- La solución deberá tener una verificación continuada de la recuperación contra problemas de integridad en la copia de seguridad inicial y/o a lo largo del ciclo de vida de los datos de la copia de seguridad.
- **La solución deberá tener capacidades de detección temprana de anomalías**.
- La solución además deberá ser compatible con sistema de inmutabilidad de tecnologías WORM de bloqueo de objetos e instantáneas de almacenamiento proporcionadas por hardware específico.
- **Es sistema de replicas debe ser del tipo "air gap", es decir deberá ser un sistema desconectado siempre, aislado, y únicamente se iniciará la conexión cuando las tareas de réplica se ejecuten.**
- **El sistema debe proporcionar mecanismos de ciber resiliencia que incluyan la comparación de las copias y la detección de cambios importantes en las**

mismas, derivados de un uso no autorizado de los sistemas a respaldar. Por tanto, deberá buscar datos con malware o corruptos con técnicas de entropía y apoyándose en motores de búsqueda de firmas como Avira o similares.

- **El sistema deberá tener capacidades de inteligencia artificial y machine learnig para detectar usos indebidos de los datos y la copias. La plataforma debe contar con funcionalidades anti-ransomware que analice el comportamiento en los servidores de producción con la utilización de archivos canarios (honeypots).**
- **El acceso a la consola de gestión de la solución se deberá implementar con múltiple factor de autenticación (MFA), bien con aplicación a teléfono móvil ,Autenticator, AuthPoint, Google, Cisco DUO u otros o con envío de uso a cuenta de correo electrónico para permitir el acceso a la consola de gestión**. o enviando correo electrónico con código de acceso a la misma.
- Las copias podrán ser cifradas por la solución. Se podrán usar múltiples algoritmos de cifrado, Blowfish, GOST, AES, Twfish, Serpent. Deberá contar con capacidad de cifrado end-to-end sin que afecte o altere la ratio de espacio optimizado por la deduplicación de las copias.
- La solución permitirá que la ejecución de determinadas tareas de gestión como el cambio de planes de copias y otras importantes requieran la aprobación entre distintos usuarios de la aplicación por lo que la aplicación deberá facilitar esta funcionalidad totalmente integrada.
- **La solución deberá mantener una copia de la base de datos de catálogo del sistema de copias en la nube del proveedor del software, lo que garantizará el acceso al sistema de copias ante contingencias graves. Esta funcionalidad deberá estar integrada en el software de copias y deberá ser configurada y administrada como parte de la solución. Se deberá permitir tener hasta 5 versiones de esta base de datos en la nube.**
- **La solución comparará las copias del Directorio Activo de Microsoft con el directorio activo de producción con el fin de detectar cambios importantes que puedan ser debidos a ataques o usos indebidos del mismo**.
- La solución comparará copias de seguridad de servidores para detectar modificaciones importantes debidas a taques en los datos.

Archivado

La solución tendrá la capacidad de archivado de todos los datos copiados, lo que permitirá liberar espacio de los servidores de producción. Esta funcionalidad se licenciará e implementará en esta licitación para las copias de datos de los dos servidores físicos antes mencionados. La solución de archivado permitirá la automatización de los procesos de archivado de datos a través de la generación de políticas y reglas que proporcionan un control total de los datos a archivar basándose en criterios específicos para su protección (tipo de dato, fecha de creación, fecha de

modificación, tamaño de archivos, etc.). El archivado deberá ser transparente para el aplicativo que usa esta información.

SUMINISTROS DE HARDWARE PARA EL SISTEMA DE COPIAS DE SEGURIDAD Y RÉPLICAS

El sistema de copias y réplicas se deberá instalar en dos servidores físicos objeto de esta licitación. Un servidor se instalará en el CPD principal de Parlamento y el segundo, para las réplicas, se instalará en el CDP secundario ubicado también en Pamplona.

Requerimientos técnicos de los servidores de copia y réplica

Ambos servidores deberán ser del mismo fabricante, misma tecnología de proceso y deberán tener los mismos niveles de soporte y servicio.

Ambos servidores deberán ser de reconocida marca comercial.

Servidor principal para copias

El servidor principal deberá tener la capacidad de poder procesar toda la carga de trabajo actual y futura, garantizando un volumen suficiente de almacenamiento para el correcto funcionamiento de la aplicación, software, índice, deduplicación, etc, y con capacidad para almacenar las copias de seguridad con la retención requerida.

Deberá tener la capacidad para que el software de copias de seguridad ofrezca las funcionalidades de inmutabilidad, que a su vez esté desligado del secundario (air gap) para evitar que se puedan propagar ataques de malware entre ambos sistemas.

Es necesario además que este hardware pueda controlar la librería LTO, y tener conectividad con la infraestructura de Parlamento de Navarra lo más rápido posible.

Por ello se propone que el hardware a adquirir en el CPD principal conste de lo siguiente:

1 servidor físico con las siguientes características mínimas:

- **Factor de forma:**
  - Servidor normalizado para rack de 19’’.
  - 1 x Chasis de 2,5” con hasta 8 discos NVMe.
- **Procesador:**
  - 2 procesadores Intel Xeon 4509Y 2,6Ghz 8 cores, 23 Mb Cache o equivalente.
- **Memoria RAM:**
  - 2 módulos de 32Gb cada uno RDIMM 5600MT/s Dual Rank.
- **Almacenamiento:**
  - 1 BOSS-N1 controller card + with 2 M.2. NVMe de 480 Gb en Raid 1.
  - 2 Discos NVMe de 960 GB cada uno en Raid 1 para índices y Base de Datos.

    - 4 Discos NVMe de 15,36 TB cada uno en Raid 6 para repositorio de copias críticas.
- **Conexión Ethernet:**
    - 1 tarjeta de red con 2 puertos ethernet de 1Gbps.
    - 1 tarjeta de red con 2 puertos 10/25 Gbps SFP28.
- **Conexión SAS:**
    - 1 tarjeta de 2 puertos SAS para conexión con LTO Scaler i3.
- **Otras conexiones:**
    - 2 USB externos mínimo.
    - 1 VGA port.
- **Alimentación**
    - 2 fuentes de alimentación de 1100W con posibilidad de ser sustituidas en caliente.
- **Unidad de expansión**
    - 1 Chasis de 3,5" con hasta 12 discos SAS/SATA/SSD.
    - 8 Discos NL-SAS de 20TB en raid 6 para repositorio del resto de copias.
    - 2 fuentes de alimentación.
    - Cables de conexión con servidor principal.
- **Otros elementos:**
    - 1 Kit de instalación en rack con pasacables para servidor y para unidad de expansión.
    - 4 cables de alimentación de 3 metros con conector macho C14 a PDU y con conector para fuente de alimentación del servidor.
    - 2 latiguillos de red de 5 metros cat. 6.
    - 2 x Cables SFP28 a SFP28 de 5 metros.
    - Cables para conectar la librería Scaler I3 a la tarjeta. Ambos puertos.
    - Puerto de Gestión externa licenciado por tiempo ilimitado para establecer mediante interfaz Web conexión a la consola local del servidor en modo gráfico.
- **S.O.:**
    - Licencia Windows Server 2022 Standard para 16 Cores.
- **Soporte y mantenimiento de fabricante**:
    - 24x7 en piezas y mano de obra durante 5 años.

Este hardware deberá ser de un fabricante de reconocido prestigio, de propósito general, pudiéndose ampliar el volumen de almacenamiento con al menos 2 discos NVME en el servidor y 4 discos NL-SAS como los indicados en la unidad de expansión.

Servidor secundario para réplicas

Al igual que en el caso del servidor principal, el servidor secundario está destinado al almacenamiento de las copias de seguridad, en este caso de las réplicas. Este servidor

irá alojado en el CPD secundario y no será necesaria la conectividad contra la librería de cintas LTO.

Al igual que en el caso del servidor principal, deberá tener la capacidad para que el software de copias de seguridad ofrezca las funcionalidades de inmutabilidad, que a su vez esté desligado del principal (air gap) para evitar que se puedan propagar ataques de malware entre ambos sistemas.

1 servidor de propósito general con la siguiente configuración mínima:

- **Factor de forma:**
  - Servidor normalizado para rack de 19''.
  - 1 x Chasis de 3,5" con hasta 12 discos SAS/SATA y 4 discos 2,5" Rear SAS/SATA
- **Procesador**:
  - 2 procesadores Intel Xeon 4509Y 2,6Ghz, 8 cores, 23M Cache o equivalente.
- **Memoria RAM:**
  - 2 módulos de 32 Gb cada uno RDIMM 5600MT/s Dual Rank.
- **Almacenamiento:**
  - 1 BOSS-N1 controller card + with 2 M.2.NVMe de 480 Gb en Raid 1.
  - 2 Discos 960 GB SSD vSAS 12 Gbps SED RI 512e 2.5in en Raid1 para índices y Base de Datos.
  - 10 Discos NL-SAS de 20 Tb cada uno en Raid 6 para repositorio de réplicas de copias.
- **Conexión Ethernet**:
  - 1 tarjeta de red con 2 puertos ethernet de 1 Gbps.
  - 1 tarjeta de red con 2 puertos 10/25 GbE SFP28.
- **Otras conexiones:**
  - 2 USB externos mínimo.
  - 1 VGA port.
- **Alimentación:**
  - 2 fuentes de alimentación de 1100W con posibilidad de ser sustituidas en caliente.
- **Otros elementos:**
  - 1 Kit de instalación en rack con pasacables para servidor y para unidad de expansión.
  - 2 cables de alimentación de 3 metros con conector macho C14 a PDU y con conector para fuente de alimentación del servidor.
  - 2 latiguillos de red de 5 metros cat. 6.
  - 2 x Cables SFP28 a SFP28 de 5 metros.

    - Puerto de Gestión externa licenciado por tiempo ilimitado para establecer mediante interfaz Web conexión a la consola local del servidor en modo gráfico.
- **S.O.:**
    - Licencia Windows Server 2022 Standard para 16 Cores.
- **Soporte y mantenimiento de fabricante**:
    - 24x7 en piezas y mano de obra durante 5 años.

PUESTA EN MARCHA DE LA NUEVA SOLUCIÓN DEL SISTEMA DE COPIAS.

PROYECTO DE PUESTA EN MARCHA

Se deberá presentar un proyecto de puesta en marcha con un cronograma que incluya al menos estas tareas:

- Reunión de planificación de trabajos a realizar.
- Instalación física. Incluirá el enracado de ambos servidores, uno en el CPD principal de Parlamento y el otro en el CPD secundario. Todo el material necesario para esta tarea deberá ser suministrado por el adjudicatario, tornillería, guías de enracado, cables de red, etc.
- Instalación del sistema operativo de los servidores de copia y réplica, Windows 2022. Actualización de los servidores con todos los parches de Microsoft. Actualización a la última versión de drivers, firmware, BIOS, otros componentes, de los servidores.
- Diseño de redes. El proyecto deberá tener en cuenta las distintas redes LAN de Parlamento para implementar la mejor y más segura puesta en marcha de la nueva solución del sistema de copias garantizando la seguridad del mismo. Se deberá hacer una propuesta a este respecto. Se deberá indicar en especial como la solución de copias implementa el “air gap” y si requiere de alguna configuración de red específica. La configuración de la electrónica de red resultante será responsabilidad el personal del Parlamento, quien acometerá esta tarea.
- Instalación del software de copias de seguridad en ambos servidores. Esto incluirá la configuración de todos los elementos que intervienen en el sistema, almacenes de datos, agentes para servidores físicos y virtuales que lo requieren, conexión con la infraestructura de virtualización para hacer las copias de las máquinas virtuales, configuraciones generales del sistema, informes, envío de alertas.
- Se deberá implementar el acceso MFA a las consolas de ambos sistemas, correo o aplicación a teléfono móvil.

- Configuración de accesos del sistema de copias a las distintas redes. El licitador deberá indicar qué configuraciones se deben abordar en el firewall que controla los accesos entre redes para permitir al software de copias acceder a la realización de copias de todas las redes. Estos accesos deberán ser los mínimos necesarios para poder hacer esta tarea exigiendo únicamente la apertura de los puertos mínimos necesarios para el acceso a la información.
- Implementación de planes de copias. Se deberá tomar como referencia para la implementación de los planes de copia la totalidad de los planes de copia señalados en el punto donde se hace referencia al sistema actual. Se deberá hacer una reorganización de los mismos atendiendo al destino en disco de los datos. Se deberá tener en cuenta que en el nuevo servidor de almacenamiento de las copias se determinan 2 tipos de disco duro con distintos niveles de rendimiento. Los sistemas que Parlamento considere más críticos se deberán implementar sobre los discos duros NVMe y el resto sobre los discos NL-SAS. Este requerimiento hará necesaria la redefinición de los planes de copia actuales. Esta tarea de reorganización de los planes obligará a duplicar alguno de los planes indicados con el fin de separar los destinos según disco y criticidad del sistema. A modo orientativo y de manera aproximada se hace una relación de totales de máquinas que irán a un tipo de disco u otro.

PLAN/ PLANES	Servidores a disco NVME	Servidores a disco NL-SAS
Máquinas físicas	2	0
Máquinas virtuales	7	7
Máquinas virtuales con agente	4	0
Máquinas virtuales semanal	6	7
Plataforma PRO admon. electrónica	8	0
Plataforma PRE admon. electrónica	0	8
Audiovisuales	0	4

Será necesario que todos los planes estén implementados y ejecutándose satisfactoriamente para considerar esta tarea del proyecto como completa.

- Se deberá configurar la librería de cintas LTO Quantum Scaler i3 propiedad del Parlamento como parte del sistema de copias en el servidor principal de copias en la sede de Parlamento. Se deberá implementar un plan de copias semanal de todas las copias de disco a cinta.
- Se deberán implementar los planes de copia a disco con este nivel de retención inicial aproximado:
    - Copia diaria. Retención de los últimos 30 días.
    - Copia mensual. Retención de los últimos 12 meses.

    - Copia anual. Retención de los últimos 5 años.
- Se deberán implementar los planes de réplica de las copias a disco con este nivel de retención.
    - Mantener las réplicas de los últimos 30 días.
    - Mantener 1 réplica de los últimos 12 meses.
    - Mantener 1 réplica de los últimos 5 años.
- Se deberán implementar los planes de copia a cinta con el siguiente nivel de retención:
    - Copia semanal. Mantener las 4 últimas semanas.
    - Copia mensual. Mantener los 12 últimos meses.
    - Copia anual. Mantener los últimos 5 años.
- Se deberá implementar la funcionalidad de archivado para los servidores físicos que son objeto de respaldar en esta licitación. Este archivado será más concretamente de un recurso compartido de uno de ellos que es utilizado como repositorio de archivos por una aplicación corporativa.
- También se deberán implementar los trabajos de réplica de las copias que hace el servidor del segundo CDP. Se deberán tener especial dedicación en el diseño lo más seguro posible del “air gap”.
- Implementación de planes de orquestación de restauraciones. Se deberán implementar planes de restauración automatizada que permitan la validación de las copias y de la restauración. Será objeto del contrato el estudio y determinación de un número limitado de servidores a modo prueba de concepto que serán objeto de esta tarea de validación del sistema de copias.
- Se deberán implementar las herramientas necesarias para poder hacer una restauración bare metal de los dos servidores físicos.
- Se deberán implementar todos los mecanismos que la solución de copias disponga para hacer una restauración bare metal de los propios servidores de copias.
- Se deberá configurar la copia a la nube del proveedor de la base de datos de catálogo.
- Se deberá indicar el procedimiento a seguir por parte de Parlamento para la restauración de esta base de datos en caso de ser necesario.
- Se deberán crear planes de análisis de vulnerabilidades de las copias. El software de backup deberá ser configurado para realizar análisis de las copias con el objetivo de detectar alteración de datos en las copias debidos a accesos no

autorizados o dañinos de la información. El licitador deberá proponer un plan de clasificación y análisis adecuado según naturaleza de los datos.

- Se deberán configurar alertas de correo y envíos de informes con resultado de ejecución de planes.
- Plan de validación. El licitador deberá presentar un plan de validación de la solución implementada que incluya:
    - La copia, restauración de al menos un par de máquinas virtuales, Windows y Linux.
    - La restauración granular de máquinas de archivos de máquinas Windows y Linux.
    - La restauración en vivo, live mount, de una máquina virtual montando la máquina virtual directamente desde el hipervisor con el almacenamiento de la copia de seguridad.
    - La restauración de máquinas desde las cintas.
    - La restauración desde la réplica de datos.
    - La restauración de algún objeto de directorio activo.
    - La restauración de algún objeto de BBDD SQL server y Postgres.
    - La realización de pruebas del comportamiento del archivado.
    - La comparación de copias de AD con el actual para detectar anomalías.

FORMACIÓN DEL NUEVO SISTEMA DE COPIAS DE SEGURIDAD Y TRASPASO DE CONOCIMIENTO

Se requerirá una formación práctica sobre la solución implementada que deberá ser impartida presencialmente por el fabricante del software, esta formación será de al menos 15 horas que se deberá distribuir en tres jornadas consecutivas, 5 horas diarias en cada jornada.

Dicha formación permitirá al personal de Parlamento de Navarra estar capacitado para la operación diaria y la resolución de los principales problemas que puedan ocurrir. Así como la capacitación para poder realizar las principales tares de copia, restauración, configuración y adecuado mantenimiento del sistema.

Esta formación deberá incluir estos contenidos:

- Componentes de la solución: Módulos que la componen.
- Consola unificada: navegación uso básico, acceso y ubicación de los servicios.
- Administración de la solución:

- Conexión a Hypervisores.
- Instalación de agentes de copia.
- Creación de planes de copias.
- Creación de planes de seguridad, monitorización activa, detección de anomalías…
- Creación de planes de orquestación de restauraciones.
- Creación de planes de archivado.
- Dissaster Recovery: protección del servidor de copias, índices, configuraciones, etc…
- Creación de planes de réplica.
- Informes, generación y envío periódico.
- Creación de usuarios.
- Securización: Implementación de MFA (Multi-Factor Authentication), y MPA (Multi-Person Authentication).
- Repositorios de datos, creación, snapshots de cabina, uso, implementación, ampliación, inmutabilidad, protección ante borrado…
- Aislamiento de la réplica, Air Gapping.

- Operativa de la solución:
  - Lanzamiento de trabajos o Jobs de copias, restauración, ciberseguridad.
  - Monitorización de trabajos: ejecución, parada, relanzamiento, logs.
  - Log de la aplicación: Principales registros, qué buscar, dónde se almacenan, retención y rotado.
  - Validación del archivado, control de qué se archiva y el ahorro generado
  - Auditado de los usuarios: acceso, acciones realizadas, borrado de datos, etc.
- Restauración:
  - Restauración de máquinas virtuales, al mismo hypervisor, u otro.
  - Restauración de ficheros de máquinas virtuales tanto Linux como Windows.
  - Restauración de elementos de BBDD (SQL server, Postgres).
  - Restauración de elementos del directorio activo.
  - Live mount. Montaje directo de la copia en el hypervisor ante desastres o ataques. Paso a producción de la copia.
- Seguridad:
  - Configuración de las distintas opciones de seguridad de la solución. Planes de alertas, detección de malware en copias, cambios en copias…
- Incidencias más comunes:
  - Detección de incidencias.
  - Solución de las incidencias.
  - Reporte y escalado a soporte.

SERVICIO DE SOPORTE Y MANTENIMIENTO DE SOFTWARE Y DEL HARDWARE

Software

Se deberán proveer las licencias de uso y soporte de la solución por un periodo de 5 años. Dichas licencias deberán proporcionar además de las funcionalidades descritas anteriormente lo siguiente:

- Acceso a la documentación oficial de la solución.
- Acceso al canal de soporte del fabricante, para poder crear incidencias.
- Actualizaciones del producto durante la vigencia de las licencias.

El soporte sobre el software será 24x7 el siguiente día laborable (NBD), debiendo ser obligatorio un canal de soporte para abrir casos de manera autónoma y directa con fabricante del software por parte de Parlamento.

Adicionalmente, en caso de que la licencia expire, **se deberá poder restaurar siempre la información protegida,** es decir Parlamento de Navarra será dueña de la información respaldada on premise.

Se deberán facilitar los canales de soporte para poder abrir casos con el fabricante del software. Deberán ser al menos:

- Portal Web.
- Teléfono.

Hardware

Todo el hardware suministrado deberá tener un soporte 24x7 in situ el siguiente día laborable (NBD) durante 5 años con el propio fabricante del hardware.

En caso de avería todos los importes de piezas, desplazamiento, mano de obra, transporte o cualquier otro tipo de servicio o suministro necesario durante la vigencia del contrato serán sin coste alguno para Parlamento.

Este soporte incluirá el acceso a nuevas versiones de firmware de los equipos suministrados para la corrección de problemas de fabricante o para la mejora y evolución de los mismos.

Se deberán facilitar los canales de soporte para poder abrir casos con el fabricante del software. Deberán ser al menos:

- Portal Web.
- Teléfono.

PERIODO DE GARANTÍA

El plazo de garantía de todos los equipos instalados será de 5 años en los términos descritos en este Anexo III, y comenzará a contarse desde la fecha de la recepción conforme de los trabajos por parte del Parlamento de Navarra.

Si durante el plazo de garantía se acreditase la existencia de vicios o defectos en los bienes suministrados e instalados, el Parlamento de Navarra tendrá derecho a reclamar del contratista la reposición de los que resulten inadecuados o la reparación de los mismos si fuera suficiente, sin cargo para el Parlamento de Navarra.

El servicio de garantía incluirá la mano de obra, material, coste de transporte, etc. asociados a la reparación de los equipos afectados, por lo que resultará sin coste para el Parlamento de Navarra.

PROPUESTA DEL LICITANTE

El licitador deberá presentar los siguientes documentos como parte de la propuesta técnica:

- El plan de implantación del proyecto, cronograma, solicitado anteriormente en este mismo documento.
- Relación de licencias ofertadas con sus correspondientes códigos, nombres comerciales y cantidades ofertadas de cada concepto.
- Dataseet software de copias.
- Certificado de fabricante de que el software ofertado cumple con la garantía y soporte solicitados, ambos para un periodo de 5 años.
- Detalle del hardware de ambos servidores. Características técnicas ofertadas.
- Certificación de fabricante de que el hardware ofertado cumple con la garantía y soporte solicitados, ambos para un periodo de 5 años.
- Dateseet hardware servidores.
- Para lo no incluido en los datseet y solicitado como requisito se deberá indicar URL de consulta en internet con el fin de verificar el cumplimiento de requisitos.
- A modo de resumen de la oferta y con carácter vinculante a la misma, se deberá cumplimentar la tabla anexo IV con las características ofertadas.