

Fondo Europeo de
Desarrollo Regional

una manera de hacer
europa 



UNIÓN EUROPEA

CONTRATO DE SUMINISTRO

ACTUALIZACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS

ACTUACIÓN COFINANCIADA POR EL FONDO EUROPEO DE
DESARROLLO REGIONAL EN EL MARCO DEL PROGRAMA
OPERATIVO FEDER MELILLA 2014-2020

PLIEGO DE PRESCRIPCIONES TÉCNICAS



MINISTERIO
DE TRANSPORTES, MOVILIDAD
Y AGENDA URBANA



Puerto de Melilla

Autoridad Portuaria de Melilla

PLIEGO DE PRESCRIPCIONES TÉCNICAS ACTUALIZACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS

Contenido

1. OBJETO	4
2. REQUISITOS DE EJECUCIÓN.....	4
2.1. Esquema Nacional de Seguridad	4
2.2. Implantación del sistema hiperconvergente.....	4
3. SITUACIÓN ACTUAL.....	5
3.1. HARDWARE	5
3.1.1. Distribución del rack 1.....	5
3.1.2. Distribución del rack 2.....	6
3.1.3. Servidores (rack 1).....	6
3.1.4. Cabinas de disco (rack 1).....	6
3.1.5. Switches CORE (rack 1).....	7
3.1.6. Switches LAN (rack 2)	7
3.2. SOFTWARE.....	7
3.3. DATASTORES	7
3.4. NETWORKING.....	7
4. ESPECIFICACIONES TÉCNICAS GENERALES.....	8
4.1. Nodos, clúster y requerimientos hardware	8
4.2. Eficiencia y cifrado de datos.....	8
4.3. Resiliencia y capacidad de almacenamiento.....	9
4.4. Gestión	9
4.5. Backup	9
4.6. Distribución de datos en modo Stretched-cluster	10
4.7. AutoSoporte y uso de inteligencia artificial para la detección precoz de incidencias	10
4.8. Dispositivo de backup externo	11
4.9. Licenciamiento	12
5. ESPECIFICACIONES DETALLADAS: HARDWARE	13
5.1. Servidores.....	13

DIVISIÓN DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

5.2.	Cabina backup	13
5.3.	Equipamiento de red.....	14
5.4.	Otros elementos.....	14
6.	ESPECIFICACIONES DETALLADAS: SOFTWARE	15
6.1.	Licenciamiento VMware.....	15
6.2.	Licenciamiento Microsoft.....	15
7.	INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN PRODUCCIÓN.....	15
8.	FORMACIÓN	16
9.	GARANTÍA.....	16

1. OBJETO

La Autoridad Portuaria de Melilla requiere la contratación de la actualización de su Centro de Procesamiento de Datos, dada la antigüedad de los sistemas que lo componen, a fin de renovar la infraestructura tecnológica primaria del Organismo (hardware y software) a un sistema hiperconvergente para mejorar el rendimiento general, conseguir un procesamiento de la información más eficiente, lograr un almacenamiento más rápido y seguro, optimizar el consumo energético, tener una mayor tolerancia a fallos, reducir costes de mantenimiento y alcanzar una mayor protección de los datos en términos de ciberseguridad.

2. REQUISITOS DE EJECUCIÓN

2.1. Esquema Nacional de Seguridad

Los accesos remotos, necesarios para la correcta ejecución del contrato por parte del adjudicatario a la Autoridad Portuaria de Melilla, exigen unas medidas de seguridad, acordes al cumplimiento del Esquema Nacional de Seguridad, que proporcionen las máximas garantías en términos de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información. Por ello, la Autoridad Portuaria de Melilla, como Organismo Público y proveedor de servicios esenciales, ha de requerir al adjudicatario la certificación de conformidad con el Esquema Nacional de Seguridad en categoría MEDIA o ALTA de sus sistemas de información que dan soporte, al menos, a la prestación de servicios de administración de sistemas.

2.2. Implantación del sistema hiperconvergente

La empresa adjudicataria deberá contar con el certificado "VMware Partner Solution Provider Data Center Virtualization".

El técnico principal del despliegue y puesta en funcionamiento del CPD deberá contar con la titulación "VMware Certified Professional Data Center Virtualization 2019" (o posterior) y contar con la experiencia mínima de haber intervenido en, al menos, dos actuaciones similares.

3. SITUACIÓN ACTUAL

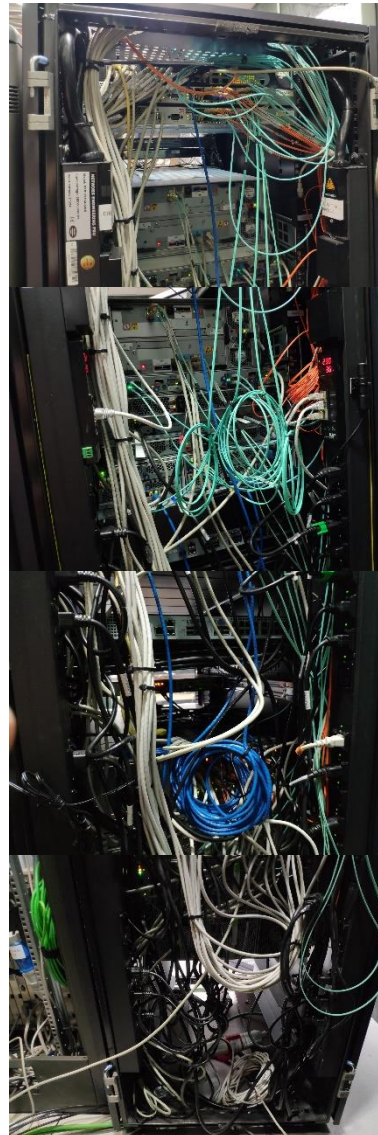
La Autoridad Portuaria de Melilla cuenta en la actualidad con un Centro de Procesamiento de Datos ubicado en una sala acondicionada de 11m² aproximadamente, con las siguientes características:

3.1.HARDWARE

3.1.1. Distribución del rack 1



Frontal



Trasera

3.1.2. Distribución del rack 2



Frontal



Trasera

3.1.3. Servidores (rack 1)

Modelo	Procesador	RAM
SUN BLADE X6270 M2	2 x Intel Xeon E5620 2.40GHz	144 GB
Sun Blade X6250	2 x Intel Xeon E5345 2.33 GHz	64 GB
SUN BLADE X4-2B	2 x Intel Xeon E5-2609 v2 2.50 GHz	384 GB
Sun Blade X6250	2 x Intel Xeon L5420 2.50 GHz	64 GB
Sun Blade X6270 M3	2 x Intel Xeon E5-2609 0 2.40 GHz	384 GB
Sun Blade X6270 M3	2 x Intel Xeon E5-2609 0 2.40 GHz	336 GB

3.1.4. Cabinas de disco (rack 1)

Modelo	Almacenamiento
Hitachi AMS 2100	6,1 TB
Hitachi HUS 110	6,3 TB
Hitachi VSP G200	23,66 TB

3.1.5. Switches CORE (rack 1)

Modelo
1 x 3com Baseline 2924-SFP Plus
2 x Brocade 200E

3.1.6. Switches LAN (rack 2)

Modelo
4 x 3com Baseline 2952-SFP Plus

3.2.SOFTWARE

Infraestructura **VMware 5.5** + VMware Data Protection, como software de backup.

Aproximadamente 75 máquinas virtuales con sistemas operativos Windows y Linux, en distintas versiones.

3.3.DATASTORES

8 datastores (LUNs) configurados con formato VMFS 5.60. Conexión fibre-channel multimodo entre servidores, cabinas y switches.

3.4.NETWORKING

4 subredes configuradas: LAN, DMZ y otras 2 dedicadas.

4. ESPECIFICACIONES TÉCNICAS GENERALES

El sistema hiperconvergente debe cumplir, como mínimo, con las siguientes características:

4.1. Nodos, clúster y requerimientos hardware

Solo serán admitidas soluciones con nodos HCI puros. Es decir, no serán admitidas soluciones desagregadas donde el cómputo y el almacenamiento estén separados.

El mismo fabricante de la solución hiperconvergente debe certificar y dar soporte sobre toda la solución en un único punto de soporte para todo el Hardware (servidores y switches) y Software (solución hiperconvergente y virtualizador VMware).

El fabricante de la solución hiperconvergente propuesta debe aportar por escrito algún tipo de garantía que asegure el cumplimiento con la implantación de la nueva solución, tales como: el porcentaje de ahorro de capacidad de almacenamiento, el tiempo en realizar un backup, el número de pasos para hacer una copia de seguridad, restauración o clonación de una máquina virtual, el tiempo en crear políticas de copia de seguridad, el tiempo de inactividad producido al quitar o añadir un nuevo nodo en la solución, etc.

El clúster de la solución debe permitir ampliación en caliente (con nodos adicionales), es decir, sin necesidad de reconfigurar el propio clúster o realizar un apagado completo, o necesidad de cambiar el licenciamiento (del software HCI) existente.

4.2. Eficiencia y cifrado de datos

La solución debe tener activados todos sus motores de eficiencia (no solo disponer de las funcionalidades). Los motores de eficiencia exigidos son Compresión, Deduplicación y Optimización de escrituras en los discos de datos. La solución podrá proveer de más motores de eficiencia, siempre que no afecten a los tres exigidos.

La solución debe tener habilitada la funcionalidad de cifrado de datos. En concreto aquella funcionalidad que permita cifrar directamente el contenido de los discos de datos. Es necesario que si un disco de datos queda expuesto (por retirada, sustitución, robo, etc.) no pueda ser 'montado' o 'accedido' por ningún otro sistema. Esta funcionalidad de cifrado debe ser ofrecida por la capa HCI, al margen de las opciones que pueda ofrecer el nivel hipervisor.

Los motores de eficiencia y el cifrado de datos deben quedar habilitados para el 100% de las cargas de trabajo y sin restricciones, ni limitaciones, entre ellos.

Dado que las funcionalidades solicitadas utilizarán los mismos recursos (CPU/RAM) que las cargas de trabajo productivas, la solución deberá identificar de forma clara la cantidad de vCPU (o Ghz) y vRAM que el software HCI consumirá en cada nodo. En

caso de que dichos consumos no sean fijos, o estén vinculados a las diferentes funcionalidades habilitadas, o no estén debidamente informadas en la documentación del fabricante, la solución deberá añadir al menos un 20% extra sobre los recursos (CPU/RAM) solicitados. La documentación entregada con la solución deberá identificar claramente este incremento de recursos (CPU/RAM).

4.3. Resiliencia y capacidad de almacenamiento

El clúster de la solución debe proporcionar un almacenamiento de alta resiliencia, similar al obtenido en una cabina de discos con doble controladora activa-activa y configuración RAID5 o superior. El almacenamiento de datos de cada nodo debe montar un RAID5 o superior para admitir la posibilidad de caída de al menos un disco en cada host.

La solución deberá realizar una protección del dato tanto dentro de cada nodo, a través de un RAID entre discos, como entre los distintos nodos que configuren cada clúster, a través de un mecanismo de réplica síncrona.

El clúster debe proporcionar los mecanismos necesarios para permitir la pérdida simultánea de 1 nodo (controlador) y al menos 1 disco de datos de cada nodo superviviente, sin que esta condición afecte a la disponibilidad de la información almacenada.

A la tolerancia de fallo descrita, ha de añadir también la capacidad de pérdida simultánea de 1 disco de estado sólido, en cada nodo que componga el clúster principal, ya sea con todos sus nodos activos o con alguno de ellos en mantenimiento.

4.4. Gestión

La solución debe estar totalmente integrada con el hypervisor VMware no siendo necesaria ninguna otra consola de gestión.

En caso de caída, pérdida o apagado de la plataforma centralizada de gestión del entorno virtualizado (vCenter), la solución debe seguir trabajando con toda normalidad, e incluso permitir acciones de backup/restore.

Al margen de la gestión integrada, la solución debe disponer de un interfaz de comandos y un interface Rest-API para cualquier integración, desarrollo de scripts o acciones en caída de la plataforma centralizada de gestión (vCenter).

4.5. Backup

Al margen de la solución de Backup externa existente, la solución debe ser capaz de auto proteger los datos, mediante funcionalidades de Backup integradas, así como de funcionalidades para realizar réplicas remotas a nodos o clúster externos.

Estas funcionalidades no deben ser tipo snapshot del hipervisor, ni snapshot de volumen, sino una funcionalidad de backup real, con granularidad de máquina virtual; es decir, sin vínculos directos con las imágenes productivas, que permitan recuperar dichas copias de seguridad incluso cuando la máquina virtual original haya sido borrada, además de permitir recuperar cualquiera de dichas copias sin afectación en la secuencia de protección. En resumen, una funcionalidad del tipo 'Full Backup'.

Las funcionalidades mínimas exigidas serán:

- ✓ Proteger y recuperar máquinas virtuales independientes (no Datastores) con sobre escritura o generando una máquina virtual nueva (GUID nuevo, etc.)
- ✓ Recuperación de ficheros y carpetas.
- ✓ Integración con VMware Tools e integración directa con VSS de las máquinas virtuales para conseguir consistencia de aplicaciones.
- ✓ Modificación de la retención de una copia específica.
- ✓ Eliminación de cualquier copia sin afectar a las secuencias de backup.
- ✓ Los RTO/RPO máximos deben estar garantizados.
- ✓ No debe limitar el uso de la solución de backup existente.

4.6. Distribución de datos en modo Stretched-cluster

De forma independiente a como sean instalados, inicialmente, los diferentes nodos que compongan la solución, será necesario que la propuesta integre las licencias/funcionalidades necesarias para establecer un modelo Stretched-Cluster para cada uno de los clústers presentados, a fin de que las ubicaciones de los nodos, y su modo de funcionamiento, puedan ser modificadas, sin incurrir en costes de licenciamientos adicionales durante su ciclo de vida.

4.7. AutoSoporte y uso de inteligencia artificial para la detección precoz de incidencias

El sistema deberá disponer de un servicio, o solución basada en Inteligencia Artificial que permita beneficiarse de todas las experiencias compartidas, de forma anónima, por otros clientes con entornos similares al ofertado.

Dicho servicio, o solución, deberá aportar informes, predicciones, recomendaciones e incluso que pueda llegar a abrir casos de soporte de forma automática y directa con el fabricante, cumpliendo, al menos, con los siguientes requisitos:

- ✓ Informes sobre el consumo de almacenamiento de cada máquina virtual.
- ✓ Informes de rendimiento del almacenamiento para cada máquina virtual.
- ✓ Monitorización del estado de salud de cada clúster presentado.
- ✓ Informes de predicción sobre el almacenamiento de la solución.
- ✓ Detección de fallo en los componentes físicos de la solución y apertura automática de incidencias con el fabricante de dichas piezas.

Estos requisitos deben ser proporcionados por la solución 'IA', de forma independiente a la información ofrecida por la propia consola del hipervisor (vCenter).

4.8. Dispositivo de backup externo

La solución debe incluir un dispositivo de Backup en ubicación secundaria. Este dispositivo debe ser un sistema de Backup a disco en formato físico.

La solución debe, de forma obligatoria, ofrecer funcionalidades para deduplicación y compresión inline (antes de la ingesta del dato), con tamaño de bloque de longitud variable; es decir, se podrá realizar la deduplicación en origen, o destino, de forma integrada con el algoritmo de deduplicación del dispositivo de Backup.

Debe admitir la recepción de datos desde ubicaciones remotas, directamente desde los servidores de aplicaciones en modo de ancho de banda bajo (deduplicación en el origen) sin requerir ningún otro elemento más allá del software, o agente, de Backup (Sin copias previas, ni optimizador WAN, etc.).

También debe permitir la replicación de bajo ancho de banda (sin rehidratar las copias), entre múltiples dispositivos de Backup, para que solo se transfieran bloques no duplicados únicos a la ubicación remota.

Las características principales deben ser:

- ✓ Un chasis rack no superior a 2U.
- ✓ Al menos 4 interfaces 10 GbE Base-T.
- ✓ Soporte para Port-Bonding (Adaptative Load Balancing & Active-Backup) y VLANs.
- ✓ Discos de sistema y datos independientes. La capacidad de los discos de sistema no será tenida en cuenta en el espacio requerido.
- ✓ Los discos de sistema utilizaran RAID1 y los discos de datos RAID6.
- ✓ Estas configuraciones RAID y Hot-Spare deben llegar configurados de fábrica.
- ✓ El dispositivo deberá permitir crecimiento hasta los 200TB de capacidad Neta.

De forma adicional, debe cumplir, al menos, con los siguientes requerimientos y funcionalidades:

- ✓ Estar certificado para trabajar con los principales ISV de proveedores de aplicaciones de copia de seguridad del mercado. Veeam, Commvault, EMC Networker, Microfocus Data Protector, NetBackup, etc.
- ✓ Gestion del Appliance basada en consola web integrada (preferible HTML5).
- ✓ Capacidad para federar múltiples Appliances para gestión unificada.
- ✓ El dispositivo de Backup propuesto también debe incluir la funcionalidad de cifrado.
- ✓ Conectores para desbordamiento de copias a "Cloud" o almacén de objetos (S3).

- ✓ Proporcionar plug-in o agentes para sistemas SAP HANA, SQL Server y Oracle.
- ✓ Admitir la emulación de repositorios VTL y NAS, tanto SMB como NFS.
- ✓ Debe proporcionar un protocolo diferente a los mencionados, que permita almacenar copias aisladas de posibles ataques Ransomware. Este protocolo, o conector, no debe ser accesible por los sistemas operativos, sino trabajar directamente con el software de Backup.

La solución de Backup externo quedará integrada, obligatoriamente, con la solución HCI, debiendo utilizar el protocolo, o conector, anti-ransomware que proporcione la solución de Backup externo. Este protocolo, o conector, no debe ser accesible, ni visible, desde los Sistemas Operativos de los clientes, o proxy, o master de backup, consiguiendo un asilamiento completo del sistema de copias de seguridad. Debe ser el propio HCI quien habilite el dialogo y transferencia de datos desde el nivel de aplicación. La integración con la solución HCI debe ser nativa, es decir, sin requerir ninguna licencia adicional, ni configuración especial que implique limitaciones en la solución HCI. A partir de esta integración, el control de copias, programación, retención, borrado, etc., deben ser gestionados desde el propio HCI, sin consola adicional.

4.9.Licenciamiento

Se deben suministrar tantas licencias como sean necesarias, en su versión más actual, completa y estable, para cubrir todos los nodos del sistema.

5. ESPECIFICACIONES DETALLADAS: HARDWARE

El adjudicatario deberá suministrar lo siguiente:

5.1. Servidores

4 Servidores *HPE Simplivity DL380 Gen10 G 15TB*, con las siguientes características:

- ✓ Formato rack, 2U de ocupación.
- ✓ Doble procesador Intel Xeon-Silver 4214R (2.4GHz/12-cores/24vCPU).
- ✓ RAM 512GB (16 x 32GB) RDIMM 2933 MHz registered memory.
- ✓ Discos de arranque: 2 x 300GB SAS 10k.
- ✓ Discos de almacenamiento: 12 discos SSD de 1,92 TB de uso mixto, extraíbles en caliente.
- ✓ 2 tarjetas de red redundantes de 10GB de doble puerto 10 GB BaseT cobre.
- ✓ 96W Smart Storage Lithium-ion Battery with 145mm Cable Kit.
- ✓ Controladora Smart Array P408i-a SR Gen10 (8 Internal Lanes/2GB Cache) 12G SAS.
- ✓ Doble fuente de alimentación intercambiable en caliente 800W Flex Slot Platinum.
- ✓ 2U Small Form Factor Easy Install Rail Kit.
- ✓ 2U Bezel Kit.
- ✓ Controladora de cifrado de datos: Smart Array SR Secure Encryption (Data at Rest Encryption/per Server Entitlement).
- ✓ Tarjeta y software de gestión remota HPE iLO Advanced.
- ✓ Cables de corriente y latiguillos de red Categoría 6A necesarios.
- ✓ Garantía y Soporte HPE: 5 años Proactive Care 24x7 Service (Tech Care Critical).

5.2. Cabina backup

1 Cabina de Almacenamiento (integrada con la infraestructura Simplivity) *HPE StoreOnce 3660 80TB Base System*, con las siguientes características:

- ✓ Formato rack, 2U de ocupación.
- ✓ Discos de almacenamiento: 10 discos de 8TB SAS 12G 7.2K.
- ✓ Capacidad: 80 TB de brutos, 56 TB (netos) útiles, ampliable hasta 200 TB.
- ✓ Licencia de encriptación StoreOnce Encryption E-LTU.
- ✓ Software Backup con compresión y deduplicación nativos, integrado con la plataforma hiperconvergente.
- ✓ 2 tarjetas de red redundantes de 10GB de doble puerto 10 GB BaseT cobre.
- ✓ Doble fuente de alimentación intercambiable en caliente 800W Flex Slot Platinum.
- ✓ Cables de corriente y latiguillos de red Categoría 6A necesarios.
- ✓ Garantía y Soporte HPE: 5 años Foundation Care 24x7 Service (Tech Care Essentials).

5.3. Equipamiento de red

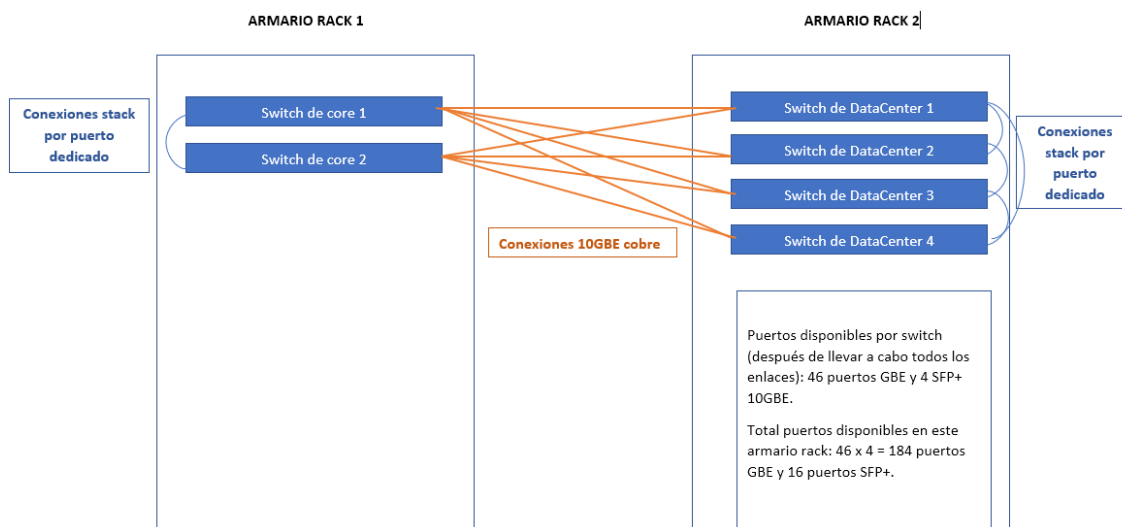
Equipamiento Core de conexionado Servidores Simplivity:

- 2 Switches *HPE 5710 24XGT 6QSFP+/2QSFP28 Switch [JL689A]* con doble fuente de alimentación y garantía/soporte HPE: 5 años Foundation Care NBD Exchange.
- 2 Cables *DAC HPE X240 100G QSFP28 3m*, para la unión de los switches en stack [JG327A].

Equipamiento DataCenter de conexionado Switches de Planta (red LAN):

- 4 Switches *Aruba 2930M 40G 8 Smart Rate PoE+ 1-slot [JL323A]* con una fuente de alimentación, un módulo de stack y un módulo de 4 puertos SFP+ por equipo, y garantía/soporte HPE: 5 años Foundation Care NBD Exchange.
- 16 Transceivers *HPE Aruba 1G SFP LC SX 500m MMF [J4858D]*.
- 4 Cables *DAC HPE Aruba 2920/2930M 3m*, para la unión de los switches en stack [J9736A].

La conexión entre los distintos switches indicados se llevará a cabo en base al siguiente diagrama:



5.4. Otros elementos

Deberán suministrarse todos los componentes y, especialmente, el cableado eléctrico y los latiguillos de cobre CAT6A y Fibra óptica multimodo que sean necesarios para el conexionado completo de todos los equipos en alta disponibilidad y correcta instalación del sistema.

El sistema ha sido diseñado por el personal técnico de la División de Sistemas de Información y Comunicaciones en base a las características funcionales y operativas descritas en el presente pliego y que se adecúan a las necesidades del Organismo en términos de calidad, rendimiento, eficiencia, durabilidad, integridad y compatibilidad; sin perjuicio de que puedan admitirse sistemas equivalentes que se ajusten a lo indicado.

6. ESPECIFICACIONES DETALLADAS: SOFTWARE

El adjudicatario deberá suministrar lo siguiente:

6.1.Licenciamiento VMware

- 1 x VMware vSphere 7 Standard Acceleration Kit for 8 processors.
- 5 años de soporte VMware 24x7: Production Support/Subscription for VMware vSphere 7 Standard Acceleration Kit for 8 processors.

6.2.Licenciamiento Microsoft

- Windows Server DataCenter (última versión publicada y estable), para los 96 cores de los 4 nuevos servidores suministrados en modalidad “Software Perpetual”.
- Windows Server User CAL, para 100 usuarios.

7. INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN PRODUCCIÓN

El adjudicatario deberá asignar un equipo de trabajo experto que reúna los conocimientos requeridos y la experiencia en la materia y sistemas objeto del contrato.

Se deberá realizar la instalación completa y despliegue de los nuevos sistemas de manera gradual, progresiva y por fases para minimizar el impacto en el funcionamiento del Organismo. Si fuera necesario una parada del sistema, se haría en horario no laboral.

De manera general, se procederá a la instalación y configuración del nuevo hardware, instalación y configuración de los S.O. correspondientes con sus licencias, migración de máquinas virtuales al nuevo entorno, retirada del hardware antiguo... y así hasta completar la puesta en producción total.

Durante el proceso de migración de máquinas virtuales se procederá a la actualización del hardware virtual y optimización de su configuración.

Se configurarán las copias de seguridad con su retención y se realizarán pruebas.

Se sustituirán todos los switches de los racks 1 y 2, se configurarán de manera óptima y se conectionarán según lo indicado.

Se instalará y configurará la cabina de almacenamiento en ubicación secundaria.

Todo el cableado, tanto el existente como el nuevo, se reorganizará, etiquetará y saneará convenientemente.

Se realizarán todo tipo de pruebas, especialmente de alta disponibilidad, para comprobar el rendimiento, la estabilidad y el correcto funcionamiento del sistema.

Todo el sistema deberá quedar configurado de manera eficiente acorde a las necesidades del Organismo.

8. FORMACIÓN

El adjudicatario deberá realizar las sesiones de formación que estime oportunas sobre el sistema implantado en su totalidad, incluyendo todo lo necesario para que el Organismo disponga de una total autonomía en la utilización, configuración, mantenimiento y resolución de posibles incidencias.

Dicha formación tendrá un carácter especializado y avanzado e irá dirigida al personal de la División de Sistemas de Información y Comunicaciones, pudiendo realizarse in situ (preferentemente) y/u online.

9. GARANTÍA

Durante el plazo de garantía establecido en el Pliego de Condiciones, el adjudicatario deberá garantizar el correcto funcionamiento del sistema de manera ininterrumpida, velando por el cumplimiento de los acuerdos de niveles de servicio (SLA) aplicables.