

Anexo II – Especificaciones técnicas del componente de Sistemas.

Contenido

1. Situación actual y objetivos.....	2
2. Esquema de la solución	2
3. Sistemas de computación	3
4. Almacenamiento	3
5. Electrónica de red.....	6
6. Backup	6
7. Licenciamiento	7
8. KVM	7
9. Servicios de Instalación y Migración	7
10. Monitorización y soporte.....	8

1. Situación actual y objetivos

El Hospital Universitario de Fuenlabrada cuenta con una infraestructura de computación integrada por una plataforma de virtualización basada en almacenamiento NetApp, servidores Cisco y software de virtualización VMware. Algunos de los equipos que forman esta infraestructura están próximos o han llegado ya a su fecha de fin de soporte por parte de los fabricantes.

Además de esta infraestructura, el hospital dispone de una serie de servidores y sistemas de almacenamiento que no se han incluido en la plataforma de virtualización, al tratarse de equipos proporcionados y soportados por sus respectivos proveedores: Archivos de imágenes (radiografías), etc.

Por otro lado, se está completando la construcción de un nuevo edificio, en el cual se ubicará un nuevo centro de proceso de datos.

El objetivo del proyecto es implantar una nueva plataforma de virtualización en dicho CPD. Esta plataforma deberá soportar toda la carga actual, además de los servicios que actualmente están corriendo en equipos independientes, no virtualizados, y disponer de capacidad de crecimiento que permita soportar nuevos requisitos y proyectos.

El proveedor deberá proporcionar el equipamiento necesario, las licencias y los servicios de instalación, configuración y puesta en servicio de la nueva plataforma; migración de las cargas de trabajo desde la plataforma actual y asistencia para la migración de las cargas de trabajo no virtualizadas, y un servicio de monitorización y soporte para la plataforma de virtualización y sus distintos subsistemas (computación, almacenamiento, backup, etc.).

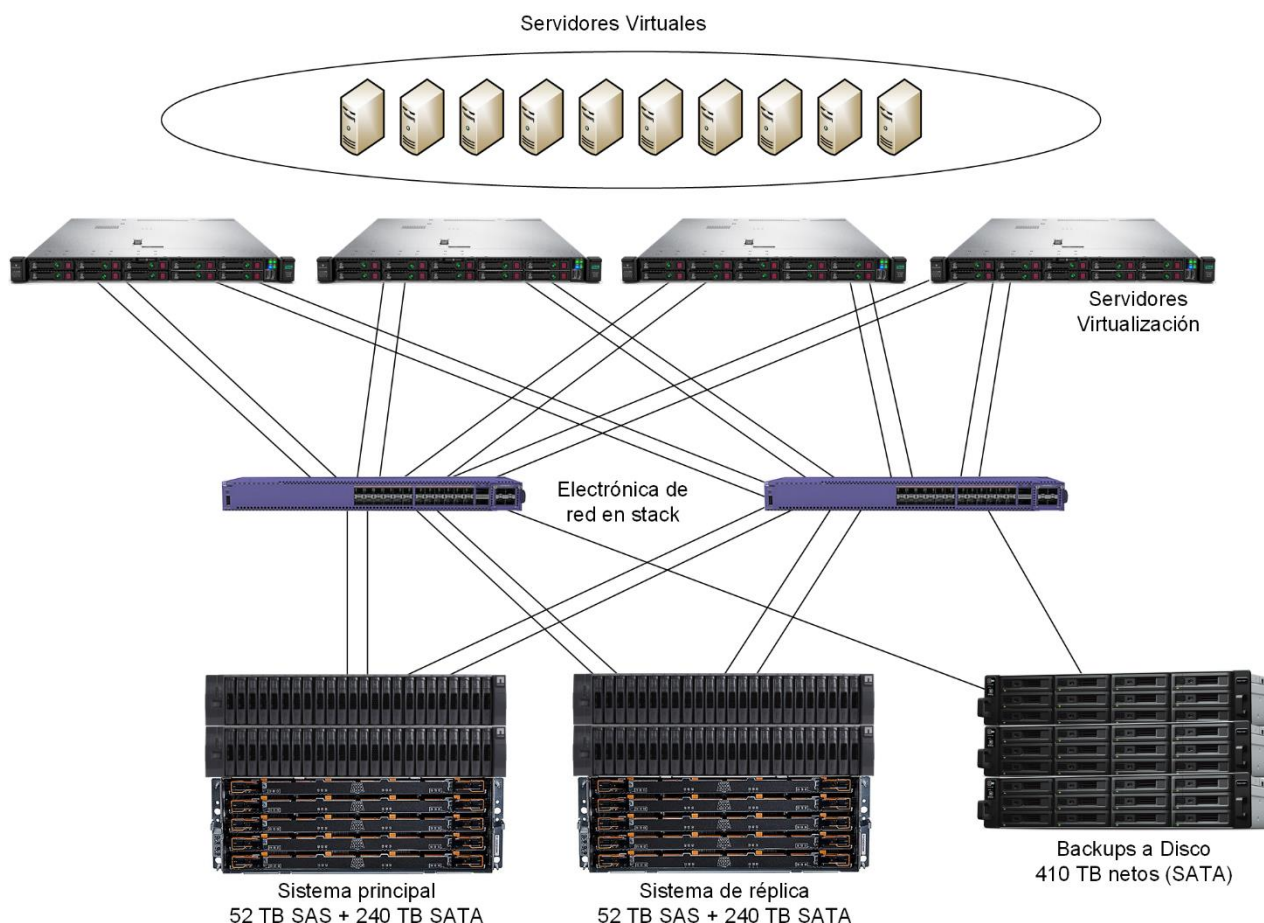
2. Esquema de la solución

El siguiente esquema muestra los distintos componentes que deben formar la solución.

El almacenamiento estará basado en dos sistemas idénticos que replicarán entre sí, de modo que en el caso de que uno de ellos fallara, se pueda migrar la producción al otro con una mínima interrupción de los servicios. Los sistemas soportarán la funcionalidad de snapshots sin pérdida de rendimiento, de tal modo que en caso de necesidad sea posible recuperar fácilmente un fichero perdido o borrado, o si es necesario una máquina virtual completa.

Los servicios de computación estarán soportados por cuatro servidores de virtualización. La conexión entre los servidores y el almacenamiento se efectuará mediante enlaces de fibra redundantes a 10 Gb. Se dispondrá de dos switches, de tal modo que, aunque falle uno de ellos no se interrumpan las comunicaciones.

El esquema incluirá un tercer sistema de almacenamiento sobre el que se realizará una copia de seguridad en disco, para lo que se emplearán las licencias de Veeam Backup & Replication de las que ya dispone el Hospital Universitario de Fuenlabrada.



3. Sistemas de computación

En la actualidad el Hospital de Fuenlabrada dispone de cuatro servidores de virtualización, que serán sustituidos por otros cuatro que deberán contar como mínimo con las siguientes características:

- 2 x Procesador Intel Xeon Silver 4314 2.4G 16 Cores, 2.4GHz, 24 MB cache.
- 1024 GB RAM (8 x 128 GB).
- 2 x 10 Gb ethernet 10Gbase-SR.
- Dispositivo de arranque en espejo.
- Fuente de alimentación y ventiladores completamente redundantes.
- 5 años de garantía y soporte 24x7.
- Deberán contar con un mínimo de 24 slots de memoria, que en caso de necesidad permita llegar a triplicar la memoria disponible.

Los servidores deberán contar con la certificación de compatibilidad con la versión de VMware vSphere que esté disponible en el momento de publicarse este pliego de prescripciones técnicas.

4. Almacenamiento

El almacenamiento deberá tener al menos las siguientes características y capacidades:

Se requiere el suministro e instalación de dos sistemas idénticos, que se configurarán como réplica uno del otro, de forma que en caso de fallo del sistema principal se pueda poner en marcha el secundario rápidamente, con una mínima interrupción de los servicios.

Los sistemas deberán soportar replicación síncrona y asíncrona integrada, sin necesidad de software ni dispositivos externos. Esto permitirá ajustarse a los requisitos de las distintas aplicaciones. Dado que el objetivo de la migración es reducir al mínimo el tiempo de interrupción de la actividad, se valorará que la replicación sea compatible con la del sistema actualmente en producción (NetApp FAS2552), con el objetivo de simplificar la migración de datos y aplicaciones.

La capacidad de cada uno de los sistemas deberá ser de al menos 290 TB netos, sin contar con ahorros obtenidos mediante de duplicación u otras funcionalidades de eficiencia de almacenamiento. De estos 290 TB, 50 TB serán en disco SAS/SSD/NVME, y el resto en disco SATA.

Cada sistema contará con dos controladoras que proporcionen alta disponibilidad, así como redundancia en todos sus componentes: Fuentes, ventiladores, puertos, etc.

Los sistemas deben ser capaces de escalar horizontalmente, añadiendo nuevas controladoras al sistema, o verticalmente, mediante nuevas bandejas hasta al menos 144 discos.

Cada controladora deberá de:

- Disponer de cuatro puertos compatibles SFP+, configurables como 1 Gb ethernet, 10 Gb ethernet u 8/16 Gb Fibre Channel mediante el cambio de SFP+.
- Incluir una caché de alto rendimiento NVMe o equivalente de al menos 1 TB.

El sistema deberá:

- Soportar e incluir licenciamiento para los protocolos FC, FCoE, iSCSI, NFS 3/4, pNFS, SMB/CIFS 3.11
- Poder crear RAIDs con doble o triple paridad que no impliquen pérdida apreciable de rendimiento.
- Incluir funcionalidades de:
 - de duplicación y compresión a nivel de bloque, inline y offline,
 - thin provisioning,
 - snapshots (hasta 1023 por volumen sin impacto apreciable en rendimiento),
 - replicación síncrona y asíncrona,
 - backup remoto,
 - gestión de calidad de servicio,
 - creación de clones instantáneos mediante snapshots escribibles,
 - recuperación instantánea de volúmenes o LUNs desde snapshots,
 - herramientas de gestión y monitorización. Administración por https o ssh.
 - envío automático de alarmas al fabricante por medio de smtp, http o https.

- Proveer una REST-API que permita la gestión y automatización de todo tipo de tareas.
- Integración con herramientas de automatización como Ansible.
- Soportar una capacidad de crecimiento hasta 144 discos, incluyendo SAS, SATA, SSD y NVME. El licenciamiento de las distintas funcionalidades deberá cubrir hasta este máximo.
- Proporcionar funcionalidades de backup basadas en snapshots consistentes por medio de integración con MS-SQL, MS-Exchange, Oracle, SAP, y otros sistemas de base de datos.
- El sistema debe ser capaz de replicar la información SAN/NAS de manera nativa con al menos 3 de los Cloud Públicos más importantes del mercado y que tengan sus datos en territorio europeo de cara al cumplimiento de normativas tipo GDPR.

Se requieren las siguientes funcionalidades de seguridad y cifrado en el sistema propuesto:

- Logs de auditoria: Capacidad de activar la recopilación de logs de acceso a los ficheros de determinadas carpetas compartidas.
- Cifrado: solución de cifrado de volúmenes de datos en reposo a nivel software, con granularidad a nivel de volumen o pool de datos, permitiendo elegir que volúmenes/pool se cifran o no, usando cifrado XTS-AES-256, y con independencia del protocolo de datos (NAS, SAN y S3), todo ello sin perder las eficiencias del dato obtenidas por los mecanismos de deduplicación y compresión.
- El sistema debe ser contar con la certificación CSfC (Commercial Solutions for Classified) o equivalente, para funcionalidades de data-at-rest (DAR).
- Posibilidad de doble factor de autenticación para conexiones SSH y CLI.
- Capacidad de uso de certificados para comunicaciones con REST API.
- Permitir IPsec data-in-flight encryption para todo el tráfico IP.
- Permitir el uso de HTTPS y SMTP como protocolo de transporte para enviar mensajes de “call home”.
- Que la replicación proporcione soporte de cifrado.
- Sistema con firewall interno para restringir el tráfico de gestión de la cabina.
- Debe soportar roles de control de acceso donde diferentes administradores tienen diferentes niveles de acceso al sistema.
- Posibilidad de requerir doble autorización por parte de un segundo administrador para la ejecución de comandos que puedan redundar en pérdida de datos.

Anti Ransomware. El sistema de almacenamiento debe incluir mecanismos de detección y prevención de Ransomware utilizando algoritmos de Machine Learning, integrados en el sistema de almacenamiento, y que analicen la actividad de los datos en los volúmenes y su entropía, para detectar ataques de Ransomware de manera automática.

- La solución Anti Ransomware debe estar totalmente integrada en las propias controladoras y software de las cabinas de almacenamiento, sin necesidad de software o URL de validación externo que haga esta función. Si una actividad anormal es detectada, se tomará un Snapshot automático de los volúmenes

afectados, el cual proporcionará un punto de restauración lo más cercano posible a la infección (RPO near zero). De manera simultánea, una alerta automática deberá ser generada y enviada a los administradores del sistema de almacenamiento y de monitorización, de manera que estos puedan determinar si la actividad es realmente maliciosa y tomar una acción correspondiente.

- Si la actividad sospechosa es un Ransomware, el sistema proporcionará en listado de los ficheros previsiblemente afectados para poder recuperarlos de manera granular sobre el Snapshot lanzado en el momento previo del ataque.

WORM. El sistema deberá permitir la creación de volúmenes NAS inmutables e imborrables para evitar que su contenido, incluyendo los snapshots, pueda ser modificado o eliminado hasta una fecha de expiración asignada. La solución deberá permitir el máximo grado de seguridad, no permitiendo ninguna operación de modificación o borrado por parte de ningún administrador que pueda comprometer los datos en WORM, no solo protegiendo a nivel de ficheros y snapshots, sino también a nivel de volumen, pool y discos.

5. Electrónica de red

Todos los componentes de la infraestructura de virtualización y almacenamiento estarán interconectados por medio de dos switches con conectividad a 10 Gb. Estos switches se configurarán como un stack que permita establecer enlaces redundantes entre los dos. En caso de fallo de uno de ellos, los equipos podrán seguir comunicándose a través de lo otro, sin provocar pérdida de servicio.

Los switches deberán proporcionar un mínimo de 24 puertos SFP+ cada uno, además de dos puertos de apilamiento con 40 Gb de ancho de banda, y posibilidad de incorporar puertos de uplink de hasta 100 Gb.

Los equipos deben ser “sin sobresuscripción”: El ancho de banda interno del equipo debe soportar que todos los puertos funcionen simultáneamente a su velocidad máxima.

Cada switch deberá contar con fuentes de alimentación y ventiladores redundantes y sustituibles en caliente.

Se deberán incluir al menos 20 SFP+ 10 Gb para la conexión de los distintos equipos. También se incluirán los SFP+ de cobre de 1 Gb y/o 10 Gb que puedan ser necesarios.

6. Backup

El sistema de backup se basará en el software Veeam Backup & Replication que ya posee el Hospital de Fuenlabrada. Se configurará un servidor virtual como servidor de backup, y las copias de seguridad de las máquinas virtuales se almacenarán en un sistema de almacenamiento cuya capacidad será de, al menos, 400 TB en discos SATA.

El sistema de almacenamiento de backup contará al menos con dos puertos 10 Gb ethernet, y deberá soportar la ampliación hasta al menos 96 discos.

7. Licenciamiento

La propuesta incluirá la actualización de las actuales licencias VMware Standard a VMware Enterprise Plus, así como el mantenimiento de estas licencias durante cinco años.

El objetivo de esta actualización de licencia es poder disponer de funcionalidades avanzadas, como son DRS y DPM (Distributed Resource Scheduler y Distributed Power Manager, respectivamente). DRS permite balancear automáticamente la carga entre los distintos servidores, mientras que DPM puede concentrar la carga en menos servidores y suspender los que no sean necesarios para ahorrar energía durante periodos de baja demanda.

También se incluirá el mantenimiento a cinco años de las licencias de Veeam Backup & Replication Standard que posee actualmente el Hospital de Fuenlabrada.

No se requiere incluir licenciamiento de Windows Server. El proyecto requiere la disponibilidad de cuatro licencias de Windows Server Datacenter, cada una licenciada para dieciséis cores, así como cuatro packs adicionales de cuatro cores, que serán aportadas por el Hospital de Fuenlabrada.

8. KVM

Se incluirá un sistema KVM con capacidad para al menos 30 equipos, y con acceso remoto vía IP, junto con el cableado y conectores necesario

9. Servicios de Instalación y Migración

Este proyecto se ha definido como un proyecto “Llave en Mano”, por lo que se incluirán todos los servicios necesarios para el despliegue y puesta en producción de la plataforma, incluyendo la migración de las máquinas virtuales desde el actual sistema al nuevo.

Entre las tareas incluidas se encuentran:

- Instalación de sistemas de almacenamiento. Actualización, creación de agregados, configuración de réplica, etc.
- Configuración de switches. Creación de stack, configuración de VLANs, interconexión con la electrónica de red del Hospital.
- Instalación de servidores. Enracado, actualización, instalación y configuración de VMware ESXi, conexión a red.
- Creación de Cluster de virtualización.
- Asignación de espacio desde sistemas de almacenamiento. Configuración de réplicas.
- Migración “en caliente” (sin interrupción de servicio) de las máquinas virtuales que están corriendo en la plataforma actual.
- Traslado de los equipos existentes que no vayan a formar parte de la plataforma de virtualización al nuevo datacenter.
- Configuración del servidor de backup. Creación de tareas.
- Configuración de alertas y sistema de monitorización.

- Pruebas del sistema.
- Documentación, transferencia de conocimiento.

10. Monitorización y soporte

Una vez completada la instalación y puesta en servicio del sistema, y aceptado el proyecto por parte del Hospital de Fuenlabrada, comenzará el periodo de mantenimiento y soporte, de acuerdo con las siguientes condiciones:

Mantenimiento Reactivo, Monitorización y soporte anual de la plataforma.

SLA: 24x7x4 en caso de parada o pérdida de servicios, 8x5xNBD para el resto de actuaciones.

Objeto del mantenimiento:

- Recuperar los servicios proporcionados por la infraestructura de virtualización del cliente en caso de parada o pérdida de servicio.
- Intervenir en caso de alertas para su resolución antes de que causen una pérdida de servicio.
- Intervención ante desastres, recuperación del servicio y de los datos desde el backup del cliente.
- Instalación en el menor tiempo posible de actualizaciones recomendadas por los fabricantes si estas son obligatorias o afectan a la seguridad.
- Instalación de actualizaciones no críticas al menos una vez al año.
- Apoyo telefónico a los técnicos del Hospital en las tareas de mantenimiento que lo precisen.

Monitorización de la plataforma de virtualización:

- Monitorización en horario de oficina, recepción de alertas 24x7.
- Recepción de notificaciones e informes de estado de los distintos componentes de la plataforma de virtualización: VMware, Veeam, Almacenamiento, servidores.
- Comprobación diaria del estado de las copias de seguridad y réplicas.

El equipamiento bajo mantenimiento será todo el que integre la plataforma de virtualización.

El Hospital proporcionará un acceso remoto a los sistemas para la correcta prestación de los servicios de monitorización, mantenimiento y soporte.

Este servicio incluirá la gestión con los distintos fabricantes para minimizar los tiempos de resolución de incidencias.

Todos los equipos y licencias incluidos en la propuesta deberán contar con sus correspondientes servicios de mantenimiento y soporte con sus respectivos fabricantes durante toda la duración del contrato.