**CIÓN**

**ANEXO 10. REQUERIMIENTOS TÉCNICOS HIPERCONVERGENCIA**

**1. SOLUCIÓN DE HIPERCONVERGENCIA**

|  |
| --- |
| **1. SOLUCIÓN DE HIPERCONVERGENCIA** |
| **ÍTEM** | **REQUISITOS ESPECÍFICOS** | **DESCRIPCIÓN DEL BIEN, SERVICIO U OBRA (ESPECIFICACIONES TÉCNICAS MÍNIMAS, MEDIDA, REFERENCIA, COLOR, ETC.)** | **CUMPLE****(SI/NO)** | **FOLIO** |
| 1 | Marca | Ofrecido por el Proponente |  |  |
| 2 | Modelo | Ofrecido por el Proponente |  |  |
| 3 | Cómputo | ***Sistema de virtualización en infraestructura Hiperconvergente***. Debe estar compuesta por recursos de cómputo, almacenamiento y gestión centralizada de forma integrada, unificada en dispositivos con arquitectura Intel x86 que aproveche los componentes locales de cada unidad y cree una plataforma distribuida con capacidad de crecimiento modular. |  |  |
| La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema puede o no incorporar elementos externos que hagan la función de testigo (witness, quorum o similar).**Nota aclaratoria**: Dado que algunas soluciones requieren un elemento externo que haga la función de testigo como otras en las que no se hace necesario. Para la Universidad de Cundinamarca son válidas cualquiera de las dos opciones. En caso de que el oferente presente la propuesta que requiera el elemento externo, éste deberá ser asumido por el oferente.  |  |  |
| 4 | Catálogo | Debe anexar el catálogo del modelo ofertado. |  |  |
| El producto ofrecido no puede estar descontinuado. |  |  |
| 5 | Calidad | La solución debe estar claramente identificada en el portal del fabricante como una solución Hiperconvergente tanto a nivel de hardware como de software. |  |  |
| 6 | Chasis | Tipo rack  |  |  |
| 7 | Nodos | * Mínimo 3 Nodos.
* Configuración en alta disponibilidad de equipos, elementos y conexiones.
* Cada nodo debe contar con su propio componente de software que se encargue de controlar el sistema de almacenamiento, que permita activar compresión y deduplicación sistemas híbridos HDD y/o SDD.
* El clúster debe poder soportar e incorporar nodos de diferentes modelos, diferentes capacidades de procesamiento, memoria, almacenamiento y diferentes familias del fabricante.
 |  |  |
| 8 | Procesador | Procesador escalable Gold o Platinum de mínimo 10 cores. |  |  |
| 9 | Velocidad Procesador | Velocidad mínima de 2,0GHz de última generación |  |  |
| 10 | Memoria RAM | DDR4-2666 o superior |  |  |
| 11 | Máquinas Virtuales | * Debe admitir la creación de máquinas virtuales Linux y Windows.
* Debe permitir Live Migration (Migración en caliente).
* Debe permitir Snapshots (Copias instantáneas) y clones para protección de datos.
* Garantizar alta disponibilidad de MV.
 |  |  |
| 12 | Soporte de Hypervisores | * El sistema híper-convergente debe incluir licenciamiento perpetuo del software de Hiperconvergencia con todas las funcionalidades (deduplicación, compresión, optimización WAN, Backup, restore, administración unificada) necesarias para hacer despliegues enterprise-class o empresariales de misión crítica, con soporte a 3 años 7x24.
* La solución (hardware) debe soportar la instalación de Hypervisores como VMWare, Microsoft Hyper-V o una distribución basada en KVM (*Máquina Virtual Basada en el Kernel*), la administración debe realizarse desde la misma consola de administración web del sistema Hiperconvergente.
 |  |  |
| 13 | Capacidad de Procesamiento Mínimo | 80 Cores |  |  |
| 14 | Capacidad de memoria RAM Mínima Efectiva | 640 GB  |  |  |
| 15 | Almacenamiento interno | * Debe soportar compresión y deduplicación.
* Mínimo 20TB Efectivas antes de compresión y deduplicación.
* Filesystem tolerante a fallas de uno o más discos.
* Filesystem tolerante a fallas por nodo de computo.
* Almacenamiento virtual compartido entre todos los nodos.
* La solución de almacenamiento no requerirá de switches de fábrica o FCoE para su funcionamiento. Solamente utilizara IP sobre Ethernet.
* La solución debe soportar exportar almacenamiento por bloques a servidores externos por medio de LUNs ISCSI y/o NFS.
* El sistema ofertado debe presentarle el contenedor de almacenamiento virtualizado al hipervisor de manera automática por medio de NFS, SMB v3.0 o iSCSI. No se aceptarán soluciones que manejen mecanismos de SAN tradicional, como LUNs, Volúmenes o grupos de discos. La solución debe tener la capacidad de distribuir los datos adentro del clúster y adicionalmente replicarlos internamente para poder asegurar su disponibilidad. Este factor de réplica debe poder ser configurado de 2 o de 3 dependiendo de las necesidades y del tamaño del clúster.
* Discos HDD 10K SFF o Discos SSD Read Intensive.
 |  |  |
| 16 | Gestión de almacenamiento (Hot Data) | Los datos más frecuentemente requeridos por una máquina virtual (Hot Data) deben estar localizados en el mismo nodo físico para asegurar el máximo desempeño, sin ser necesaria una configuración especial a nivel de hipervisor o del almacenamiento, esta funcionalidad la debe controlar automáticamente el software de Hiperconvergencia de forma nativa. |  |  |
| 17 | Disco Cache | * El sistema de almacenamiento debe tener disco de cache de estado sólido.
* Los datos más frecuentemente requeridos por una máquina virtual (Hot Data) deben estar localizados en el mismo nodo físico.
 |  |  |
| 18 | Interfaces | * 1 Tarjeta 10GB Dual SFP Network Adapter. Debe incluir los dos (2) SFP (Transceivers) con licenciamiento para conexión con los puertos del switch TOR (Top of the Rack).
* Cada nodo debe contar como mínimo con 2 puertos Ethernet 10GbE UTP para tráfico de Administración, Back Up y Replica.
 |  |  |
| 19 | Accesorios  | El equipo debe contener todos los cables, módulos y rieles requeridos para su instalación, configuración, funcionamiento.  |  |  |
| 20 | La solución de Hiperconvergencia debe tener funcionalidades de compresión y deduplicación.  |  |  |
| 21 | La solución debe detectar de manera proactiva el daño de como mínimo un (1) disco, removerlo automáticamente del clúster y reconstruir de manera inmediata los datos que ahí́ se alojen en los otros discos del clúster. En caso de que el disco sea removido o se encuentre en estado fuera de línea (offline), la reconstrucción de los datos también debe iniciarse de manera automática e inmediata.  |  |  |
| 22 | La solución debe distribuir los datos en el almacenamiento interno del clúster y adicionalmente replicarlos internamente para poder asegurar su disponibilidad. |  |  |
| 23 | La solución de Hiperconvergencia deberá proveer un crecimiento modular y escalable, garantizando el aprovisionamiento tanto de cómputo, memoria y almacenamiento. |  |  |
| 24 | En el mismo nodo donde se encuentra la máquina virtual, debe estar el almacenamiento virtualizado, permitiendo entregar los recursos I/O requeridos por la máquina virtual local en cada nodo, inclusive en caso de migración de una máquina virtual a otro nodo. |  |  |
| 25 | El sistema de Hiperconvergencia debe contar con mecanismos de eficiencia de espacio como Erasure Coding, Compression y/o Deduplication tanto para clúster con almacenamiento híbridos (SSD y HDD) como para almacenamientos All-flash indistintamente. |  |  |
| 26 | La solución debe soportar exportar almacenamiento por bloques a servidores externos por medio de LUNs, ISCSI y/o NFS |  |  |
| 27 | La solución Hiperconvergente con su hipervisor nativo debe proveer recuperación granular de archivos protegidos por Snapshots y/o Backups y esta funcionalidad debe poder entregarse como auto-servicio a los usuarios de las VMs sin requerir la adquisición de productos adicionales del fabricante o de terceros |  |  |
| 28 | La solución debe soportar el respaldo y restauración de copias de las máquinas virtuales y archivos hacia la nube pública.  |  |  |
| 29 | El portal de auto aprovisionamiento debe estar construido sobre una interfaz web y ser administrado a través de navegadores como Chrome, Firefox, Safari o Internet Explorer.  |  |  |
| 30 | El portal de auto aprovisionamiento debe soportar la integración con el directorio activo para el manejo de la autenticación de los usuarios del mismo. |  |  |
| 31 | El portal debe permitir la creación de roles de usuarios con diferentes privilegios. |  |  |
| 32 | La solución debe proveer alta disponibilidad haciendo uso de las diferentes formas de replicación. |  |  |
| 33 | El sistema debe ofrecer la capacidad de mantener consistente la replicación de un grupo de volúmenes y/o máquinas virtuales de tal manera que los Snapshots y/o Backups se tomen en el mismo punto en el tiempo.  |  |  |
| 34 | El sistema debe proveer la capacidad de programar la toma periódica de Snapshots y/o Backups a máquinas virtuales. |  |  |
| 35 | El sistema debe soportar la creación de un disco virtual cuya capacidad es mayor a la capacidad disponible en el nodo en que reside. Todas las tecnologías de Alta Disponibilidad y protección de datos con que cuente la solución deben estar disponibles para un disco virtual con ésta característica. |  |  |
| 36 | El sistema debe hacer que todos los SSD instalados estén disponibles como medio de almacenamiento primario, y no solamente para almacenar metadatos o para hacer cache |  |  |
| 37 | El sistema debe incluir una funcionalidad que notifique automáticamente al fabricante acerca de condiciones de error de manera proactiva. |  |  |
| 38 | La solución Hiperconvergente debe soportar autenticación de dos factores para la consola gráfica de administración. |  |  |
| 39 | La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de Hiperconvergencia instalada como un servicio en cada uno de los nodos que componen la solución manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información. |  |  |
| 40 | La solución debe permitir entregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y Discos, así como IOPS de lectura, IOPS de escritura, y latencias.  |  |  |
| 41 | La solución debe permitir el análisis de ancho de banda utilizado por la misma así como el ancho de banda de una máquina virtual. |  |  |
| 42 | La solución debe proveer accesos alternativos basados en SSH. |  |  |
| 43 | La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, firmware de los nodos e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni indisponibilidad del servicio. |  |  |
| 44 | El fabricante de la solución ofertada deberá estar calificado como líder en el cuadrante mágico de Gartner del año 2018 para infraestructura Hiperconvergente.  |  |  |
| **2. SOLUCIÓN SWITCH CORE REDUNDANTES** |
| 1 | Marca | Ofrecido por el Proponente |  |  |
| 2 | Modelo | Ofrecido por el Proponente |  |  |
| 3 | Cantidad | Dos (2) |  |  |
| 4 | Unidades de Rack | Switch de tipo top of Rack, mínimo 1 unidad de Rack,  |  |  |
| 5 | Fuente de Poder | Cada Switch debe incluir fuente de poder de backup hot swappable |  |  |
| 6 | Interfaces SFP+ | Cada Switch debe incluir mínimo 20 interfaces SFP+ 1G, 10G o 40G |  |  |
| 7 | Transceivers SFP+ | Cada Switch debe incluir siete (7) transceiver SFP+ 10GB (Fibra) de acuerdo al numeral **3.1.2 DIAGRAMA LÓGICO DE CONEXIÓN SOLUCIÓN DE HIPERCONVERGENCIA.**  |  |  |
| 8 | Soporte de puertos | Cada Switch debe incluir Soporte de puertos universales de 1G, 10G o 40G |  |  |
| 9 | Puertos Ethernet | Cada Switch debe incluir mínimo tres (3) puertos a 10GbE (cobre) y tres (3) puertos a 1GbE (cobre) de acuerdo al numeral **3.1.2 DIAGRAMA LÓGICO DE CONEXIÓN SOLUCIÓN DE HIPERCONVERGENCIA.**  |  |  |
| 10 | RAM | RAM mínima 4 GB |  |  |
| 11 | Soporte de Virtual Chassis | Mínimo 6 unidades |  |  |
| 12 | Interfaces 100% Non-Blocking |  |  |
| 13 | Switch Fabric igual o superior a 640Gbps |  |  |
| 14 | Soporte de virtualización de red mediante SPB y/o MPLS |  |  |
| 15 | Soporte de Ventilación Front-to-back. |  |  |
| 16 | Soporte de Listas de control de acceso (ACL) |  |  |
| 17 | Protección avanzada de trama IPv6 (DHCP Snooping, protección de anuncio de router y protección source address Filter) que proporciona protección frente a una amplia gama de ataques de suplantación de direcciones |  |  |
| 18 | Capacidad de trabajar los estándares para Data Center DCB (Data Center Bridging), PFC (Priority Flow Control 802.1Qbb), ETS (Enhanced Transmission Selection - IEEE 802.1Qaz), EVB (Edge Virtual Bridge - 802.1Qbg) |  |  |
| 19 | Capacidad de agregación de enlace IEEE 802,3ad (LACP) hasta 16 enlaces en el mismo agregado. |  |  |
| 20 | Soporte a protocolos de enrutamiento RIP v1/v2, RIPng, OSPFv2, OSPFv3, BGPv4 instalados y operativos |  |  |
| 21 | Soporte de IGMPv2, IGMPv3 Snooping, PIM-SM y DVMRP en IPv4 y MLD en IPv6 instalados y operativos |  |  |
| 22 | IEEE 802.1D, Spanning Tree Protocol |  |  |
| 23 | IEEE 802.1P QoS |  |  |
| 24 | IEEE 802.1Q VLAN Tagging  |  |  |
| 25 | IEEE MVRP |  |  |
| 26 | IEEE 802.1AB LLDP  |  |  |
| 27 | IEEE 802.1s MSTP  |  |  |
| 28 | IEEE 802.1w RSTP |  |  |
| 29 | IEEE 802.3ad Link aggregation |  |  |
| 30 | IEEE 802.3x |  |  |
| 31 | IEEE 802.3az (Energy Efficient Ethernet) en todo sus puertos |  |  |
| 32 | Soporte de IEEE 802.1x múltiples hosts y múltiples vlans por puerto |  |  |
| 33 | Autenticación flexible de dispositivos y usuarios con IEEE 802.1x/MAC |  |  |
| 34 | Protección embebida con un motor de denegación de servicio (DoS) incorporado para impedir los ataques del tráfico no deseado |  |  |
| 35 | Debe incluir DHCP Server IPv6 e IPv4 |  |  |
| 36 | Soporte de SNMPV3. |  |  |
| 37 | Soporte de Administración vía web. |  |  |
| 38 | Soporte de Administración 100% vía CLI y SSHv2. |  |  |
| 39 | Temperatura de operación mínima 0°-45° C |  |  |
| 40 | Humedad (funcionamiento y almacenamiento) mínimo 10% — 90% (non-condensing) |  |  |
| 41  | Los equipos conectados en modo stacking o virtual chasis, deben comportarse como una sola unidad lógica, una sola dirección IP, si requiere hardware adicional o licencias adicionales deben estar incluidos en la oferta. |  |  |
| **2.1 SISTEMA DE GESTION SWITCH CORE REDUNDANTES** |
| 1 | Marca | Ofrecido por el Proponente |  |  |
| 2 | Modelo | Ofrecido por el Proponente |  |  |
| 3 | Cantidad | 1 |  |  |
| 4 | El sistema de administración ofrecido deberá utilizar interfaces gráficas de usuario, basado en WEB. |  |  |
| 5 | Debe estar licenciada para gestionar los Switches incluidos en la oferta. |  |  |
| 6 | La función de gestión centralizada debe permitir la configuración y la copia de seguridad y restauración de software por equipo, así como la copia de seguridad y restauración masivos. |  |  |
| 7 | Mediante el sistema ofrecido se deberá permitir actualizar el firmware de los Switches adquiridos en este proyecto, de manera individual o conjuntamente por modelos o referencias específicas. |  |  |
| 8 | Mediante el sistema ofrecido se deberá realizar, el respaldo de las configuraciones de cada uno de los Switches adquiridos en este proyecto.  |  |  |
| 9 | Deberá permitir monitoreo de tráfico a nivel de puertos físicos de los Switches. |  |  |
| 10 | Debe permitir personalizar la información mostrada en la página inicial. |  |  |
| 11 | Deberá permitir el envío automático de correos electrónicos al administrador en el caso de la ocurrencia de eventos críticos. |  |  |
| 12 | Deberá incluir todos los módulos para generar reportes gráficos de Consumo de Red hasta el nivel 7 de aplicación. |  |  |
| 13 | Debe incluir todos los módulos para generar reportes gráficos de TopN Users, Top N Switch, Top N ports y Top N Applications |  |  |
| 14 | Deberá permitir la gestión de cuarentena de equipos por puerto y dirección MAC en los equipos. |  |  |
| 15 | Debe permitir establecer inventario de dispositivos. |  |  |
| 16 | Debe permitir la búsqueda y localización de usuarios en la red tanto LAN por dirección IP, MAC y usuario de dominio |  |  |
| **3. SISTEMA DE RESPALDO (HARDWARE Y SOFTWARE)** |
| 1 | Marca | Ofrecido por el Proponente |  |  |
| 2 | Modelo | Ofrecido por el Proponente |  |  |
| 3 | Cantidad | 1 |  |  |
| 4 | Capacidad mínima | 24 TB efectivo:* Discos HDD 10K SFF o Discos SSD Read Intensive SFF
 |  |  |
| 5 | RAM mínima | 32 GB DDR4-2666 |  |  |
| 6 | Puerto de administración. | 1 |  |  |
| 7 | RAID | Mínimo 5 |  |  |
| 8 | Puertos 1000Base-T | Mínimo 2  |  |  |
| 9 | Puertos SFP+ | Mínimo 2, con transceiver SFP+  |  |  |
| 10 | Fuente de poder | Redundante (incluida) |  |  |
| 11 | Sistema Operativo | Incluido y Licenciado |  |  |
| 12 | DD adicionales | Entrega de dos (2) discos mínimos como repuesto a la solución ofertada |  |  |
| 13 | Tipo de Procesador | Procesador Gold o Platinum de mínimo 10 cores, velocidad mínima 2,2 GHz de última generación.*Capacidad de procesamiento mínimo:* 10 cores |  |  |
| 14 | La solución debe tener la capacidad de poder gestionar de manera centralizada tareas de respaldo y replica. Administrada por cualquiera de los siguiente Hypervisores: VMWare o Hyper-V o KVM.  |  |  |
| 15 | La solución deberá tener la capacidad de establecer parámetros de cifrado a los archivos de respaldo dentro de un repositorio.  |  |  |
| 16 | La solución debe tener la capacidad de importar archivos de respaldo tomados con la misma instancia u otra y proveer la capacidad de restaurarlos luego de ser importados.  |  |  |
| 17 | La solución deberá contar en la interface web con información del estado de protección de las máquinas virtuales, trabajos de respaldo, repositorio de respaldo, logs de eventos y la salud general del servidor de respaldo.  |  |  |
| 18 | La solución debe proveer la capacidad de generar archivos de respaldo de la configuración dando de igual manera la opción de restaurar la misma.  |  |  |
| 19 | La solución deberá proveer mecanismos de compresión y deduplicación para los trabajos de respaldo y optimizar la utilización de disco.  |  |  |
| 20 | Deberá tener la posibilidad de generar tareas de respaldo por máquina virtual y en adición grupos de protección definidos previamente  |  |  |
| 21 | Deberá establecer parámetros de ejecución automática estableciendo calendarización y retención definida para los trabajos de respaldo.  |  |  |
| 22 | La solución deberá incluir la capacidad de activar bajo demanda las tareas de respaldo establecidas y en adición generar respaldos completos (Full) incluyéndolos en la cadena de respaldos.  |  |  |
| 23 | La solución deberá contar con la capacidad de copiar los respaldos en otra localidad, utilizando políticas de retención paralelas.  |  |  |
| 24 | Deberá poder gestionar las recuperaciones de máquinas virtuales completas a la localidad original o una diferente definiendo el punto de restauración dentro de la cadena de respaldo.  |  |  |
| 25 | Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de servicio de directorio, tales como, Microsoft Active Directory, pueden utilizar para recuperar objetos individuales, tales como usuarios, grupos, directivas de grupos (GPO), registros de DNS, particiones de configuración. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.  |  |  |
| 26 | Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Microsoft SQL Server, puedan recuperar objetos individuales, tales como tablas y registros. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma  |  |  |
| 27 | Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Oracle 11.x o superior, puedan recuperar bases de datos sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma  |  |  |
| 28 | Deberá incluir herramientas de fácil recuperación de elementos granulares como: sitios, archivos, librerías, carpetas sin la necesidad de recuperar todo el respaldo o agente para Microsoft SharePoint 2010 en adelante.  |  |  |
| 29 | Deberá incluir una herramienta de fácil recuperación a nivel de archivo para los diferentes sistemas operativos sin la necesidad de restaurar todo el archivo de respaldo.  |  |  |
| 30 | Deberá disponer de funcionalidades integradas que permitan la selección de un destino de almacenamiento de respaldos que pueda estar alojado en un proveedor de servicios en la nube (BaaS).  |  |  |
| 31 | La solución deberá proporcionar alertas e informes por correo electrónico de la situación y ejecución de los trabajos de respaldo.  |  |  |
| 32 | Deberá ofrecer un conjunto de reportes capaz de presentar información de tipo:1. Reportes que permitan la planificación de la capacidad.
2. Reportes que permitan la determinación de inefectividad en el uso de recursos.
3. Reportes que faciliten la visibilidad de tendencias negativas y anomalías.
4. Tableros de control claros, presentables e integrables en sitios web.
5. Envío automático y programado de reportes de auditoria para operaciones de recuperación y modificaciones a políticas de respaldos o replicación.
 |  |  |
| 33 | Deberá poseer la capacidad de generar segregación de acceso según el perfil del usuario, al monitoreo de la infraestructura conectada a la plataforma.  |  |  |
| 34 | Deberá ofrecer la capacidad de reportar el cumplimiento de políticas de protección de datos y disponibilidad acorde a parámetros definidos.  |  |  |
| 35 | Envío de notificaciones de alarmas cuando se detecten configuraciones erróneas o problemas potenciales en la infraestructura del respaldo.  |  |  |
| 36 | Soporte para reportes de respaldos de agentes físicos de la solución.  |  |  |
| 37 | La plataforma debe contener reportes genéricos tales como:1. Historia de las tareas de respaldo
2. Reportes de máquinas protegidas, físicas y virtuales
3. Reporte de actividad de recuperación de datos
4. Reporte de verificación de recuperabilidad
5. Ultimo estado de tareas de respaldo
6. Resumen de alarmas de respaldo
7. Reporte de configuración de Infraestructura virtual
8. Reporte de respaldos en cintas
9. Reporte de máquinas en cumplimiento
10. Inventario de Respaldo
 |  |  |