Gobernación de Cundinamarca

ANEXO 9.

REQUISITOS TÉCNICOS NUEVA INFRAESTRUCTURA DE HYPERCONVERGENCIA.

Tabla de contenido

1. ARQUITECTURA SOLICITADA: 7
1.1. DATACENTER PRINCIPAL: 7
1.2. DATACENTER ALTERNO: 8
2. CAPACIDAD DE LOS NODOS DE HYPERCONVERGENCIA: 8
3. CAPACIDAD SERVIDOR DE BACKUP DATACENTER PRINCIPAL: 9
4. EXPANSIÓN LIBERÍA DE CINTAS LTO9: 10
5. CAPACIDAD SW´S DATACENTER PRINCIPAL: 10
6. LIBRERÍA DE CINTAS LTO8: 10
7. LICENCAMIENTO VMWARE: 11
8. ESPECIFICACIONES NODOS DE HYPERCONVERGENCIA: 11
9. ESPECIFICACIONES SERVIDOR DE BACKUP: 22
10. ESPECIFICACIONES LIBRERÍA DE BACKUP: 27
11. ESPECIFICACIONES SW´s: 29
12. EVALUACIÓN DE LA SOLUCIÓN OFERTADA: 33

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

PRESENTACION

El presente documento contiene las características técnicas requeridas por el Departamento de Cundinamarca – Secretaría de Hacienda, para la renovación tecnologica de la solución de Hyperconvergencia.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

DEFINICIONES

- **Hyperconvergencia (HCI):** Es un enfoque de infraestructura de TI que integra cómputo, almacenamiento y red en un solo sistema gestionado por software, utilizando la virtualización.
- **Nodo:** Es un servidor físico o virtual dentro de un clúster o entorno informático distribuido que está específicamente diseñado para realizar tareas de computación.
- **Discos para boot (arranque):** Es cualquier dispositivo de almacenamiento, como un disco duro, unidad de estado sólido (SSD) o pendrive, que contiene los archivos necesarios para iniciar el sistema operativo de una computadora.
- **SO:** Son las siglas de Sistema Operativo, que es el software fundamental que actúa como intermediario entre el hardware del dispositivo (computadora, teléfono, etc.) y el usuario o las aplicaciones.
- **BaseT:** Es un cable Ethernet que utiliza par trenzado como método de cableado. "Base" indica que se utiliza transmisión en banda base, mientras que "T" indica que se utiliza un cable de par trenzado.
- **QSFP+:** (Quad Small Form-Factor Pluggable Plus) es un tipo de puerto en dispositivos de red de alta velocidad que permite la transmisión de datos a 40 Gbps utilizando 4 canales de 10 Gbps.
- **Virtualización:** Es una tecnología que crea múltiples entornos informáticos simulados (o virtuales) a partir de un único sistema físico, como un servidor, un dispositivo de almacenamiento o una red.
- **Librería de Backup:** (también conocida como biblioteca de cintas o jukebox) es un dispositivo de hardware para el almacenamiento automatizado de datos en cintas magnéticas.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- **Expansión (Modulo) Librería:** Es un componente de hardware que se utiliza para aumentar la capacidad de almacenamiento. Estos módulos permiten la adición de más slot y de más drives para mejorar la eficiencia de la toma de backups.

- **NVMe:** (Non-Volatile Memory Express). Es un protocolo de comunicación diseñado para aprovechar la velocidad del bus PCI Express (PCIe) y conectar unidades de almacenamiento SSD (unidades de estado sólido) directamente a la CPU.

- **Drive o Unidad LTO:** Es un dispositivo de almacenamiento en cinta magnética que utiliza el formato Linear Tape-Open (LTO) Ultrium para copias de seguridad, archivado y transferencia de grandes volúmenes de datos.

- **Deduplicación de Datos:** Es una técnica que minimiza el espacio requerido para almacenar datos. Se ha diseñado para ayudar a las organizaciones a abordar el problema de los datos duplicados. Con independencia de que una empresa acumule varias copias del mismo archivo o de varios archivos que contengan los mismos datos, la deduplicación sustituye las copias adicionales de datos con metadatos que simplemente apuntan al original.

- **DAC (Direct Attach Cable):** Es un tipo de cable de cobre de alta velocidad y corta distancia que se utiliza para conectar equipos de red como servidores, switches y routers.

- **Ethernet SFP+:** Enhanced Small Form Factor Pluggable (Factor de Forma Pequeño Enchufable mejorado) y es la versión mejorada de SFP. proporciona velocidades de datos de hasta 16 Gbit/s.

- **RAID:** (Matriz Redundante de Discos Independientes). Es una tecnología que combina varios discos duros en un único sistema lógico para mejorar el rendimiento o la fiabilidad de los datos, o ambos.

- **RFP:** (Request for Proposal), o Solicitud de Propuesta, es un documento formal que una organización emite para solicitar propuestas a proveedores potenciales sobre cómo pueden cumplir con un proyecto, servicio o adquisición específica.

- **GPU:** (Graphics Processing Unit) o unidad de procesamiento gráfico es un circuito electrónico especializado que acelera la creación de imágenes, vídeos y otros gráficos.

- **OEM:** (Original Equipment Manufacturer). Se refiere a un fabricante de equipo original en inglés. Es una compañía que produce piezas o componentes que otra empresa utiliza para ensamblar un producto final, que luego se vende bajo la marca de esa segunda empresa.

- **WAN:** (Wide Area Network, o Red de Área Amplia en español) es una red informática que conecta múltiples redes más pequeñas (como las LAN) a través de grandes distancias geográficas, como ciudades o países, facilitando la comunicación y el intercambio de información a escala global.

- **ISV:** (Proveedor de Software Independiente, por sus siglas en inglés). Es una empresa que desarrolla y vende software propio, el cual funciona en el hardware y los sistemas operativos de otras compañías.

- **RTO:** (Objetivo de Tiempo de Recuperación). Es el tiempo máximo aceptable para restablecer las operaciones de un sistema o aplicación después de una interrupción, con el fin de minimizar las pérdidas comerciales y el impacto en la empresa.

- **RPO:** Significa tanto Objetivo de Punto de Recuperación como Externalización de Procesos de Reclutamiento.

- **FIPS:** son las siglas de Federal Information Processing Standards (Estándares Federales de Procesamiento de Información), un conjunto de normas de ciberseguridad creadas por el gobierno de EE. UU. para proteger datos y sistemas sensibles.

- **Runbook:** Es un documento o conjunto de instrucciones detalladas que describe paso a paso cómo realizar una tarea específica o un conjunto de tareas dentro de las operaciones de un sistema informático.

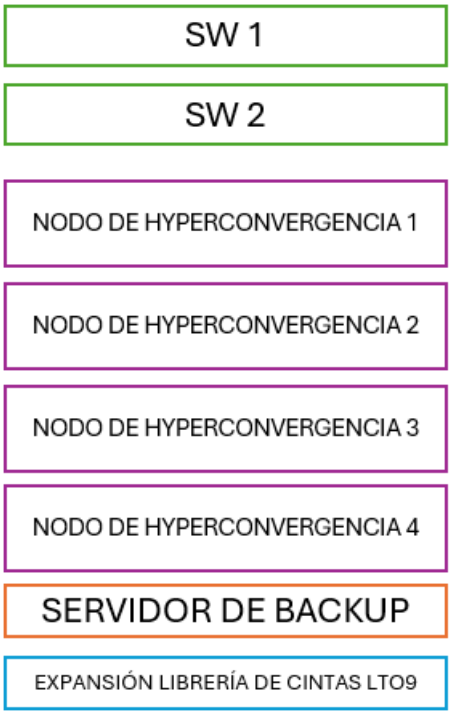
- **SAS:** (Serial Attached SCSI). Es una interfaz de conexión de alta velocidad para dispositivos de almacenamiento, diseñada para servidores empresariales, que reemplaza al antiguo estándar SCSI paralelo.

- **SATA:** (Serial Advanced Technology Attachment). Es una interfaz de transferencia de datos en serie que conecta dispositivos de almacenamiento, como discos duros.
- **SSD:** (unidad de estado sólido). Es un dispositivo de almacenamiento de datos que utiliza memoria flash y circuitos integrados para almacenar información de manera persistente, sin partes mecánicas ni discos giratorios como los discos duros (HDD) tradicionales.
- **HBA:** (Host Bus Adapter). Es una placa de circuito o un adaptador de circuito integrado que conecta un sistema host, como un servidor, a un dispositivo de almacenamiento o de red
- **Hot Spare:** Es un disco de almacenamiento o componente de sistema que se mantiene en espera y alimentado para reemplazar automáticamente un disco o componente que falle, activándose de forma instantánea y sin intervención del usuario para mantener el sistema operativo y los datos seguros y operativos.
- **Infiniband:** es un estándar de comunicación de red de alto rendimiento diseñado para centros de datos, clústeres de supercomputadoras y aplicaciones de inteligencia artificial.
- **UEFI:** (Interfaz de Firmware Extensible Unificada). Es el firmware moderno y avanzado que reemplaza a la antigua BIOS, encargándose de la inicialización del hardware y el arranque del sistema operativo.
- **Cintas LTO (8-9):** (Linear Tape-Open). Son un formato de almacenamiento de datos en cinta magnética, desarrollado por IBM, HP y Seagate, diseñado para backups, recuperación de desastres y archivo de grandes volúmenes de información a largo plazo.

1. ARQUITECTURA SOLICITADA:

El Departamento de Cundinamarca Secretaría de Hacienda requiere la siguiente arquitectura para la hacer la renovación tecnologica de la solución de hyperconvergencia:

1.1. DATACENTER PRINCIPAL:

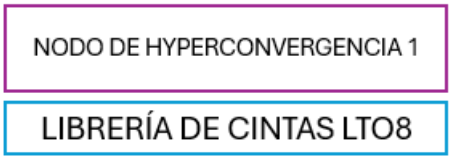


En el Datacenter principal se requiere:

- 2 SW de 48 puertos, configurados en redundancia y alta disponibilidad, para conectar los 4 nodos de hyperconvergencia.
- 4 nodos de Hyperconvergencia.
- Un servidor de Backup.
- Expansión de dos drives LTO9 FC a la Librería de Backup HPE MSL3040 S/N DEC31508FR: En la actualidad se cuenta con 3 drives LTO8.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

1.2. DATACENTER ALTERNO:



En el Datacenter alterno se requiere:

- 1 nodo de Hyperconvergencia.
- Una librería de Backup LTO8 SAS.

2. CAPACIDAD DE LOS NODOS DE HYPERCONVERGENCIA:

Datacenter Principal:

La capacidad que deben cumplir cada uno de los nodos de hyperconvergencia debe ser

- Memora RAM: 3 TB.
- Discos para boot: (2) 480 GB NVMe M.2 SSDs en RAID 1.
- Disco: 31 TB usables.
- Procesadores: 2 procesadores de 2.9 GHZ, de 24 cores cada procesador.
- Tarjetas de red: una tarjeta de 1Gb de 4 puertos BaseT, dos tarjetas de 10Gb de 2 puertos BaseT.
- Fuentes de poder redundantes que soporten el normal funcionamiento de nodos.
- Soporte de fabricante con partes y/o repuestos a 5 años en modalidad 7*24 - 4 horas en atención.
- Servicios de instalación de fabricante en horario no hábil.
- Se deben proveer todos los cables para asegurar su correcto funcionamiento
- Licenciamiento SO: Microsoft Windows Server 2025 Datacenter para la totalidad de los cores.

Datacenter Alterno:

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

La capacidad que deben cumplir el nodo de hyperconvergencia debe ser

- Memora RAM: 3 TB.
- Discos para boot: (2) 480 GB NVMe M.2 SSDs en RAID 1.
- Disco: 31 TB usables.
- Procesadores: 2 procesadores de 2.9 GHZ, de 24 cores cada procesador.
- Tarjetas de red: una tarjeta de 1Gb de 4 puertos BaseT, dos tarjetas de 10Gb de 2 puertos BaseT.
- Fuentes de poder redundantes que soporten el normal funcionamiento de nodos.
- Soporte de fabricante con partes y/o repuestos a 5 años en modalidad 7*24 - 4 horas en atención.
- Servicios de instalación de fabricante en horario no hábil.
- Se deben proveer todos los cables para asegurar su correcto funcionamiento
- Licenciamiento SO: Microsoft Windows Server 2025 Datacenter para la totalidad de los cores.

3. CAPACIDAD SERVIDOR DE BACKUP DATACENTER PRINCIPAL:

La capacidad que deben cumplir el servidor de Backup del Datacenter principal debe ser:

- Memora RAM: 256 GB
- Discos para boot: (2) 480 GB NVMe M.2 SSDs en RAID 1.
- Disco: 19,2 TB RAW.
- Procesadores: 2 procesadores de 2.6GHz, de 8 cores cada procesador.
- Tarjetas de red: una tarjeta 1Gb de 4 puertos BaseT, una tarjeta 10Gb de 2 puertos BaseT.
- Tarjetas de red Fibra: 4 tarjetas de 2 puertos 32Gb.
- Fuentes de poder redundantes que soporten el normal funcionamiento del servidor.
- Soporte de fabricante con partes y/o repuestos a 5 años en modalidad 7*24 - 4 horas en atención.
- Servicios de instalación de fabricante en horario no hábil.
- Se deben proveer todos los cables para asegurar su correcto funcionamiento
- Microsoft Windows Server 2025 Standard para la totalidad de los cores.

4. EXPANSIÓN LIBERÍA DE CINTAS LTO9:

Datacenter Principal:

En la actualidad la Entidad tiene una librería de cintas HPE MSL3040 S/N DEC31508FR con tres (3) drives fibra LTO8, se requiere ampliar en dos (2) drives fibra LTO9. Se deben entregar 2 cajas de 20 cintas LTO9 de 45TB RW.

Este un equipo con soporte de fabricante hasta el 22/09/2026, se debe asegurar el soporte a 5 años de la librería y los dos drives de expansión requeridos.

5. CAPACIDAD SW´S DATACENTER PRINCIPAL:

Datacenter Principal:

Se requieren dos SW con las siguientes capacidades:

- 48p 10GBASE-T.
- 6 puertos QSFP+.
- Fuentes de poder redundantes.
- Se deben proveer todos los cables para asegurar su correcto funcionamiento.
- Soporte de fabricante con partes y/o repuestos a 5 años en modalidad 7*24 - 4 horas en atención.

6. LIBRERÍA DE CINTAS LTO8:

Datacenter Alterno:

- Una librería que soporte mínimo 3 drivers.
- Un drive LTO8 SAS
- 1 caja de 20 cintas LTO8 de 30TB RW
- Soporte de fabricante con partes y/o repuestos a 5 años en modalidad 7*24 - 4 horas en atención.
- Se deben proveer todos los cables para asegurar su correcto funcionamiento.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

7. LICENCAMIENTO VMWARE:

En la actualidad la Entidad utiliza la herramienta de virtualización VMWare, para facilitar la migración de los ambientes administrados de la plataforma actual de hyperconvergencia y a la nueva plataforma que entregará el operador, se requiere mantener la misma herramienta de virtualización.

Por lo anterior se debe ofertar el licenciamiento de VMware vSphere Foundation o su sustituto por 5 años para la totalidad de los cores de la nueva solución.

No obstante, la Entidad aceptará propuestas que contemplen otras herramientas de virtualización equivalentes, siempre que estas garanticen la correcta migración y operación de los entornos virtualizados requeridos. En estos casos, la responsabilidad de la migración y puesta en funcionamiento de los ambientes será asumida por el contratista.

El oferente deberá indicar en su propuesta la herramienta de virtualización ofrecida para un periodo de cinco (5) años, especificando el modelo de licenciamiento (perpetuo o por suscripción) y adjuntando la ficha técnica oficial de la solución propuesta.

8. ESPECIFICACIONES NODOS DE HYPERCONVERGENCIA:

La solución propuesta debe basarse en una plataforma de infraestructura de TI convergente que integre almacenamiento, computación, redes, hipervisor, deduplicación en tiempo real, compresión y optimización junto con potentes capacidades de administración de datos, protección de datos y recuperación ante desastres en un bloque de construcción de servidor x86 estándar.

REQUISITOS DE HARDWARE Y RENDIMIENTO:

- Cada nodo debe proporcionar 48 núcleos, 3.072GB de RAM utilizable y 30 TB de almacenamiento utilizable.
- Cada nodo debe admitir hasta dos procesadores escalables Intel Xeon de última generación, con capacidad de 8 a 56 núcleos por nodo.
- Cada nodo debe permitir la actualización de fábrica de uno a dos procesadores.
- Cada nodo debe admitir la memoria inteligente registrada DDR4-2xxx de última generación.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Cada nodo debe permitir la actualización de fábrica de RAM hasta 1536 GB por procesador y escalar a 3 TB por nodo.
- La solución hiperconvergente debe configurarse utilizando un disco duro de no más de 3.84 TB.
- Cada nodo debe tener cuatro puertos Ethernet de 1 GbE integrados y cuatro puertos Ethernet SFP+ de 10/25 GbE con opción de fibra óptica, DAC de cobre o RJ45.
- Cada nodo debe tener una administración fuera de banda integrada para simplificar la administración remota.
- Cada nodo debe tener uno o más controladores RAID de 12 GB para administrar las unidades dentro del nodo.
- Cada nodo debe tener al menos 3 ranuras PCI disponibles y también debe admitir al menos un adaptador de GPU.

Almacenamiento en caché y resiliencia:

- El dispositivo HCI propuesto debe contar con un 5 % adicional de espacio utilizable para el almacenamiento en caché de escritura, ya sea en unidades dedicadas o distribuido en las unidades de datos ofrecidas en una partición independiente.
- El espacio de caché propuesto deberá configurarse en alta disponibilidad y ser compatible con al menos dos fallos de unidad por nodo.

Eficiencia de datos:

- El dispositivo HCI propuesto debe ser capaz de deduplicar, comprimir y optimizar todos los datos en línea, en tiempo real, en todos los niveles de almacenamiento para operaciones de escritura desde las máquinas virtuales.
- La eficiencia de los datos se gestionará con una granularidad de bloques de datos de 4 KB u 8 KB.
- La deduplicación y la compresión deben ser completamente en línea, lo que significa que deben realizarse antes de que la solicitud de escritura de la máquina virtual llegue al disco de datos o al disco de caché disponible en un nodo determinado.
- La falla de un disco en el nodo HCI no deshabilitará la deduplicación y la compresión de un nodo determinado, ni temporal ni permanentemente.
- La deduplicación y la compresión utilizarán el tamaño de bloque de datos unificado para todo el conjunto de datos de la máquina virtual para garantizar la eficiencia de los datos y no superarán los 8 KB.
- La deduplicación y la compresión estarán siempre habilitadas, independientemente de la naturaleza de los datos, sin afectar el rendimiento.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- La deduplicación y la compresión se realizarán en línea, independientemente del tipo de E/S, como operaciones secuenciales o aleatorias.

Hipervisor:

- La solución hiperconvergente debe ser compatible con los principales hipervisores de la industria.
- El hipervisor debe ser de propósito general y no propietario. El hipervisor debe ser compatible tanto con HCI como con entornos no HCI, utilizando las licencias adecuadas.
- El hipervisor debe ubicarse en discos que no formen parte del almacenamiento principal de datos.

Expansión

- La solución hiperconvergente debe permitir la actualización de CPU, RAM y capacidad de almacenamiento desde el equipo, así como la expansión horizontal.
- La solución hiperconvergente debe poder comenzar con un mínimo de 2 nodos para lograr alta disponibilidad y escalar horizontalmente cuando sea necesario.
- La solución hiperconvergente debe admitir la adición de nodos de solo cómputo/acceso (sin almacenamiento de datos) para proporcionar recursos computacionales adicionales y debe ser compatible con servidores de todas las marcas OEM como CN (nodos de cómputo).
- La solución hiperconvergente ofrecida debe admitir la gestión al menos 96 nodos en una única federación.

Resiliencia

- La solución propuesta debe ser capaz de soportar múltiples puntos de fallo en varios nodos, sin pérdida de funciones ni datos.
- La solución propuesta se ofrecerá con una combinación de hardware para fallos de disco en cada nodo, y los fallos de nodo deberán estar protegidos al menos con RF2 (Factor de Replicación 2).
- Si el proveedor no ofrece protección contra fallos de disco a nivel de hardware en un nodo determinado, deberá proporcionar la protección completa del nodo con RF3 (Factor de Replicación 3).
- Cada nodo deberá contar con dos fuentes de alimentación (PSU) dedicadas, no compartidas, y ser capaz de soportar fallos de una sola fuente de alimentación. La

solución no deberá utilizar una arquitectura de microservidor con PSU compartidas ni otros componentes.

- Debe ser capaz de soportar obligatoriamente un mínimo de fallos simultáneos de un disco duro en cada nodo del clúster y en todos los nodos del clúster sin pérdida de datos.
- La solución ofrecida también debe ofrecer la flexibilidad para soportar fallos simultáneos de dos discos duros en cada nodo del clúster y en todos los nodos del clúster sin pérdida de datos durante la implementación.
- Cada nodo ofrecido debe ser capaz de soportar un fallo de puerto NIC.

REQUISITOS DE SOFTWARE Y FUNCIONALIDAD

Funciones comunes incluidas:

- La solución hiperconvergente debe tener una eficiencia de datos garantizada de 10:1 al gestionar datos y copias de seguridad de máquinas virtuales locales, o bien, el OEM de HCI debe proporcionar por escrito el compromiso de eficiencia de datos.
- La plataforma hiperconvergente ofrecida debe ser compatible con copias de seguridad, recuperación y recuperación ante desastres (DR) basadas en políticas para cada máquina virtual. Se debe proporcionar todo el software necesario, como el de copias de seguridad, si se. requiere
- La plataforma hiperconvergente ofrecida debe ser compatible con la protección de datos optimizada para la WAN para la movilidad de las máquinas virtuales. Solo la información única debe fluir a través de la WAN después de habilitar la deduplicación y la compresión. Todos los accesorios necesarios para habilitar la deduplicación y la compresión a través de la WAN deben estar incluidos en la solución. Las funciones de optimización de la WAN deben estar integradas en el dispositivo HCI ofrecido.
- Los datos no deben rehidratarse antes de transferirse al centro de datos de destino
- La solución hiperconvergente deberá tener soporte integrado para la interfaz de almacenamiento de contenedores (CSI) y deberá estar calificada para funcionar con plataformas de contenedores basadas en Kubernetes de código abierto.

Gestión Unificada Global

- La solución hiperconvergente ofrecida deberá permitir la gestión centrada en máquinas virtuales (VM) a través de un único panel mediante el administrador de virtualización del hipervisor correspondiente.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- El administrador de virtualización del hipervisor correspondiente deberá ser capaz de gestionar uno o varios clústeres a través de una única consola de gestión.
- El dispositivo hiperconvergente ofrecido deberá ser capaz de gestionar todos los aspectos de la hiperconvergencia para todos los sitios a través del administrador de virtualización de un Hyper-Converge determinado.
- El hiperconvergente ofrecido deberá ser capaz de exponer/conectarse a los servidores existentes del cliente para alojar máquinas virtuales y aplicaciones, aprovechando al máximo la funcionalidad de la solución.
- El hiperconvergente ofrecido deberá ser capaz de gestionar globalmente las políticas de backup por almacén de datos o por máquina virtual y controlarlas directamente a través del administrador de virtualización del hipervisor correspondiente.
- La solución hiperconvergente deberá contar con una única consola de gestión de actualizaciones para simplificar la actualización del software hiperconvergente, el hipervisor y la capacidad de revertir las actualizaciones anteriores.

Habilitado para la nube: monitoreo, inteligencia artificial e integración de hipervisor

- Integración del motor de análisis y monitoreo habilitado para la nube con Hypervisor
- El motor de monitoreo y análisis habilitado para la nube ofrecido debe estar estrechamente integrado con la capa de hipervisor ofrecida y debe estar certificado para funcionar con al menos VMware.
- La integración en la nube debe ser capaz de proporcionar monitoreo de extremo a extremo de múltiples centros de datos, múltiples clústeres de HCI, almacenes de datos, host de hipervisor y máquinas virtuales que se ejecutan dentro del centro de datos.
- Cualquier licencia necesaria para monitorear múltiples clústeres desde una sola consola se proporcionará en las instalaciones o en la nube. Para evitar cualquier límite, el proveedor proporcionará las licencias de losa más altas de la gestión de múltiples clústeres.
- La herramienta de monitoreo e integración en la nube debe tener un mecanismo incorporado con el equipo de soporte de back-end para el registro automático de casos de soporte de condiciones de error definidas.
- La herramienta de monitoreo e integración en la nube debe tener la capacidad de identificar las principales máquinas virtuales que contribuyen al máximo consumo de E/S y espacio.
- La herramienta de monitoreo e integración en la nube mostrará el estado del contrato de soporte en cada nivel de controlador virtual / nodo.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- La herramienta de monitoreo e integración en la nube debe mostrar la tendencia del consumo de capacidad para el uso pasado y futuro para una planificación efectiva de la capacidad.
- La herramienta de supervisión e integración en la nube estará estrechamente integrada con las copias de seguridad de datos locales y remotas y mostrará desde una única consola las copias de seguridad locales y remotas de todas y cada una de las máquinas virtuales.
- La herramienta de supervisión e integración en la nube mostrará el coeficiente de eficiencia de la capacidad general y destacará claramente los índices de deduplicación y compresión por separado.
- En caso de que el proveedor no admita la funcionalidad ofrecida anteriormente en la nube, se ofrecerá la misma funcionalidad en las instalaciones con la versión empresarial del software de gestión de proveedores con licencias ilimitadas para administrar múltiples clústeres y funcionalidades de copia de seguridad empresarial.

Copia de seguridad y protección de datos:

- La funcionalidad de copia de seguridad y protección de datos será una característica integral de Hyper-Converge en lugar de una licencia de servidor / software separada
- La copia de seguridad debe ser una copia independiente del servidor virtual de origen y debe permitir la restauración del servidor virtual de origen eliminado o dañado.
- La copia de seguridad independiente no debe usar ni depender de la tecnología de instantáneas del hipervisor proporcionado.
- La copia de seguridad integral debe tener la capacidad de definir la política de copia de seguridad por almacén de datos, un grupo de máquinas virtuales o una máquina virtual específica
- La copia de seguridad integral debe tener la capacidad de ejecutar tareas de copia de seguridad en un intervalo específico, como un día específico de la semana o un día del mes.
- La copia de seguridad integral debe tener flexibilidad para retener la copia de seguridad crítica o marcada durante un período prolongado de tiempo en meses y años. Admitirá la retención de datos de respaldo al menos durante 10 años sin utilizar ningún software adicional.
- La copia de seguridad integral debe tener la capacidad de ejecutar tareas de copia de seguridad durante el horario de oficina sin afectar las cargas de trabajo de producción.
- El cluser Hyper-converge ofrecido será realmente flexible y admitirá de forma nativa hasta 2 millones de copias de seguridad diarias.
- La solución propuesta debe ser capaz de proporcionar informes de respaldo con fines de auditoría

- La solución de hiperconvergencia debe tener un tiempo de copia de seguridad del clúster local garantizado de > = 5 minutos.
- La copia de seguridad integral proporcionará el panel de control para las copias de seguridad fallidas.
- La solución de hiperconvergencia ofrecida proporcionará la flexibilidad completa para la copia de seguridad a nivel de máquina virtual en lugar de forzar la protección a nivel de almacén de datos o dominio de protección.
- La solución de copia de seguridad integrada ofrecida tendrá flexibilidad para cambiar la política de vencimiento de la copia de seguridad a nunca para un archivo de copia de seguridad determinado para una mayor retención.
- La solución de copia de seguridad integrada ofrecida deberá ser capaz de hacer copias de seguridad de los volúmenes persistentes del contenedor.
- La solución de hiperconvergencia ofrecida proporcionará la flexibilidad completa para clonar máquinas virtuales específicas.

Infraestructura de respaldo y protección de datos.

- Proporcionar la solución de copia de seguridad requerida (ya sea incorporada) o adicional para los requisitos de copia de seguridad anteriores.
- El Vendedor se asegurará de que el motor de respaldo se ejecute en cada nodo HCI ofrecido.
- Si el proveedor necesita crear una máquina virtual separada para las operaciones de copia de seguridad y recuperación, el proveedor se asegurará de que la máquina virtual se cree en cada nodo de HCI ofrecido en HA.
- El Proveedor también podrá integrar el dispositivo de copia de seguridad basado en disco dentro del clúster dado de forma nativa mientras mantiene la deduplicación y la compresión.
- El proveedor podrá utilizar un dispositivo basado en disco tanto para la copia de seguridad local como para la copia de seguridad a través de WAN sin ninguna puerta de enlace adicional.
- El Vendedor podrá realizar la inmutabilidad de los datos de copia de seguridad mientras envía los datos al dispositivo de copia de seguridad basado en disco.
- En caso de que el proveedor no pueda realizar una integración nativa del dispositivo de copia de seguridad basado en disco.

Restauración (recuperación de datos).

- La recuperación de datos debe ser independiente del servidor virtual de origen

- Será posible buscar el trabajo de copia de seguridad utilizando varios parámetros para una máquina virtual determinada utilizando el tiempo de caducidad, el nombre del clúster, la marca de tiempo de la copia de seguridad, etc.
- La solución ofrecida proporcionará la capacidad de verificar el tamaño único de la copia de seguridad antes de iniciar la operación de restauración
- La solución ofrecida permitirá la restauración de la máquina virtual reemplazando la máquina virtual de origen existente, la creación de una nueva máquina virtual o la restauración en un centro de datos diferente dentro del hipervisor.
- La solución ofrecida deberá poder copiar el archivo de copia de seguridad junto con los metadatos en diferentes clústeres como una característica nativa del software de copia de seguridad y restauración.
- La solución hiperconvergente debe proporcionar un catálogo de copia de seguridad para permitir que cualquier máquina virtual se recupere en cualquier punto específico en el tiempo
- El proceso de recuperación de datos debe ser simple con un RTO en minutos para un clúster determinado**.**

Replicación de datos

- La solución ofrecida debe admitir la capacidad de llevar a cabo una replicación bidireccional simultánea entre dos centros de datos
- La plataforma ofrecida deberá tener la capacidad de replicar Cualquiera a Cualquiera en una implementación de centro de datos de malla de más de 3 centros de distribución.
- La replicación entre ubicaciones se realizará en modo de ancho de banda bajo y utilizará tecnologías de deduplicación y compresión mientras se replican los datos.
- La solución ofrecida deberá tener capacidad para limitar el ancho de banda de replicación

Seguridad:

- La solución propuesta debe ser capaz de proporcionar cifrado de datos At_Rest para una mayor seguridad de los datos
- La solución propuesta deberá tener la capacidad de permitir la gestión de claves desde una única consola para la solución de gestión de claves local y externa

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Recuperación ante desastres (conmutación por error y conmutación por recuperación):

- Se basará en la protección continua de datos, brindando soporte tanto para la protección local como remota.
- Admitirá capacidades de copia de seguridad y recuperación ante desastres on premises, on premises DR y en nubes pública como Azure y AWS.
- Será una herramienta de orquestación y automatización de la resiliencia de TI, capaz de proporcionar informes de SLA y monitoreo de RPO en todo momento.
- Proporcionará conmutación por error y recuperación automáticas tras iniciar la ejecución de la recuperación ante desastres según las políticas definidas.
- Podrá generar alertas automáticas si el nivel de RPO supera el límite establecido.
- Podrá proteger incluso las máquinas virtuales críticas de gran tamaño que utilizan más de 120 vCPU.
- Podrá admitir discos RDM de más de 60 TB tanto en modo físico como virtual.
- Proporcionará una herramienta crítica para resistencia a ransomware: detección de anomalías de cifrado en tiempo real.
- La detección de cifrado por ransomware estará integrada en el software, sin necesidad de herramientas adicionales.
- Deberá contar con la capacidad nativa integrada de replicación permanente (Always on Replication) en lugar de utilizar la tecnología de snapshot/clonación, tanto para la protección de datos locales como para la recuperación ante desastres (DR).
- No deberá tener ningún agente de software dentro de las máquinas virtuales de producción proporcionadas.
- Deberá tener la flexibilidad necesaria para proporcionar un RPO inferior a 10 segundos tanto para la protección de datos local como para la protección de datos remoto, excluyendo la latencia del enlace.
- Deberá ser capaz de crear miles de puntos de control, separados por menos de 10 segundos, para un RPO y RTO mínimos utilizando tecnología basada en registros o equivalente.
- Deberá tener la capacidad de crear grupos de aplicaciones consistentes para aplicaciones multi-VM, lo que garantizará la coherencia de los datos durante la copia de seguridad y la recuperación.
- Deberá tener la capacidad de definir el orden de arranque de las máquinas virtuales dentro del grupo de aplicación consistente durante la operación de conmutación por error para reducir el RTO general.
- No deberá imponer ninguna limitación en el número de grupos consistentes de la aplicación, o el proveedor deberá admitir al menos 256 grupos consistentes de la aplicación para la consistencia de los datos.

- No deberá imponer ninguna limitación en el número de máquinas virtuales dentro de los grupos consistentes de la aplicación, o el proveedor deberá admitir al menos 2048 máquinas virtuales dentro de los grupos consistentes de la aplicación para la consistencia de los datos.
- Deberá poder priorizar la replicación del tráfico de máquinas virtuales dentro del grupo de consistencia de la aplicación según las necesidades de la organización en los niveles bajo, medio y alto, y deberá realizar un uso automático del ancho de banda.
- Deberá ser compatible con tecnologías de optimización de WAN, como la compresión, para proteger la información en la ubicación de recuperación ante desastres.
- Deberá tener la capacidad de activar/desactivar la tecnología de optimización WAN en función del tipo de máquinas virtuales o del grupo de aplicaciones.
- Deberá admitir la inmutabilidad para la retención cuando se utilice almacenamiento compatible con S3 on premises, Amazon S3 o Azure.
- Deberá poder definir la inmutabilidad para copias de retención completas y también deberá tener la flexibilidad de definir, para una aplicación determinada, un grupo de consistencia en el software.
- Deberá tener la capacidad de realizar failover desde la ubicación principal a la ubicación de recuperación ante desastres en modo automatizado, de modo que no sea necesario crear la máquina virtual manualmente en la ubicación de recuperación ante desastres.
- Deberá tener la capacidad de seleccionar el punto de restauración o punto de control, según los requisitos de la organización, al realizar la conmutación por error desde la ubicación principal a la ubicación de recuperación ante desastres.
- Deberá tener la capacidad de seleccionar el orden de arranque de la máquina virtual en la ubicación de recuperación ante desastres durante el proceso de conmutación por error para minimizar el tiempo de recuperación total.
- Deberá tener la capacidad de configurar la protección inversa (de la ubicación de recuperación ante desastres a la ubicación principal) después de un failover exitoso de la ubicación principal a la ubicación de recuperación ante desastres.
- Deberá tener una política de confirmación flexible para que el entorno pueda revertirse a la ubicación principal si el failover de recuperación ante desastres planificada no se realiza correctamente debido a un evento imprevisto o a cualquier motivo desconocido.
- Deberá contar con una política de confirmación flexible, con plazos que van desde minutos hasta horas, de modo que, tras el failover, las operaciones puedan comprobarse exhaustivamente antes de anunciar que la conmutación se ha realizado correctamente.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Para failover planificado, la política de faiolver deberá proporcionar al cliente la flexibilidad necesaria para apagar el entorno virtualizado del sitio principal con un RPO mínimo.
- Deberá contar con un sólido mecanismo de protección contra el ransomware y deberá lograrse con un RPO mínimo.
- Deberá tener la capacidad de crear un punto de control cada 5 segundos de protección de datos, de modo que el cliente pueda seleccionar el punto de control necesario al restaurar los archivos durante un ataque de ransomware y pueda lograr el RPO más bajo.
- Deberá tener la capacidad de almacenar la información más reciente, al menos durante un mes, en los dispositivos de almacenamiento más rápidos (NVMe o SSD) y la información del día restante en los medios más lentos de forma automática. Esto garantiza una recuperación rápida tras un ataque de ransomware.

Seguridad del sistema y soporte remoto

- Para la seguridad del firmware, el sistema hiperconvergente debe admitir un chip de administración remota que cree una huella digital en el silicio, evitando que el sistema se inicie a menos que el firmware coincida con la huella digital. Esta característica debe ser inmutable
- Debe mantener un repositorio para recetas de firmware y controladores en la unidad flash asociada al puerto de administración. Esto es para ayudar a revertir o parchear el firmware comprometido. También debe almacenar la receta de recuperación de fábrica precargada para revertir al firmware seguro probado de fábrica
- La administración remota del sistema hiperconvergente debe admitir la consola remota gráfica basada en navegador junto con el botón de encendido virtual, el arranque remoto mediante una unidad USB / CD / DVD.
- El sistema hiperconvergente debe admitir la administración sin agente mediante el puerto de administración remota fuera de banda.
- El sistema hiperconvergente debe admitir el uso compartido de consolas remotas de hasta 6 usuarios simultáneamente durante la operación previa al sistema operativo y al tiempo de ejecución del sistema operativo

Soporte:

- Organización de soporte mundial establecida que puede proporcionar soporte local y remoto hasta 24x7, 365, 4 horas de tiempo de respuesta

- Soporte mundial establecido que puede proporcionar soporte L3 para productos de hiperconvergencia que pueden proporcionar soporte de resolución desde el hipervisor hasta el hardware.

Licenciamiento:

- Todo el Hyerconverge ofrecido tendrá licencia con deduplicación en tiempo real, compresión, hipervisor, al menos 4 implementaciones multisitio, licencia automatizada de conmutación por error y conmutación por recuperación, software de copia de seguridad (incorporado o externo según el requisito de funcionalidad RFP) y licencia de consola de administración empresarial para administración de múltiples clústeres.
- En caso de que el proveedor necesite proporcionar una licencia adicional para lograr las funcionalidades solicitadas, se incorporarán

9. ESPECIFICACIONES SERVIDOR DE BACKUP:

Chasis: Montaje en rack de 2U.

CPU: Uno o dos números de procesador escalable Intel® Xeon® de 4ª generación de 32/36/40/44/48/52/56 núcleos.

Chipset: Chipset Intel® C741.

Memoria:

- Ranuras 32DIMM.
- DIMM de xx GB escalable hasta 8,0 TB mediante DIMM registrado DDR5 (RDIMM) que funciona a 4800 MT/s

Bus Slots:

- El servidor debe admitir hasta tres ranuras PCI-Express 5.0 x16.
- Dos ranuras PCIe 5.0 x8 o superiores adicionales

BOOT optimized storage: 2 x 40GB M.2 NVMe Hot Plug Boot Optimized Storage en RAID 1

HDD Bays:

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Cambio en caliente 8 SFF SAS/SAT/SSD/NVMe

Controller:

- El servidor debe admitir uno de los siguientes controladores, debe admitir el modo mixto que combina el funcionamiento del modo RAID y HBA simultáneamente:
- Controlador RAID x16 integrado / basado en PCIe con caché de escritura respaldada por Flash de 8 GB, compatible con RAID 0, 1, 5, 6, 10, 50, 60.
- Debe admitir unidades SAS, SATA y NVMe combinadas en la misma controladora. El controlador debe ser compatible con 6G SATA, 12G SAS, 16G NVMe. o Controlador RAID x16 integrado / basado en PCIe compatible con RAID 0, 1, 10.
- Debe admitir unidades SAS, SATA y NVMe combinadas en la misma controladora. El controlador debe ser compatible con 6G SATA, 12G SAS, 16G NVMe. o Controlador RAID integrado / basado en PCIe con caché de escritura respaldada por flash de 4 GB compatible con RAID 0, 1, 5, 6, 10, 50, 60 s
- Debe admitir unidades SAS, SATA y NVMe combinadas en la misma controladora. El controlador debe ser compatible con 6G SATA, 12G SAS, 16G NVMe.

El controlador mencionado anteriormente debe admitir lo siguiente:

- Raíz de confianza de hardware y cifrado y descifrado seguro de datos críticos de la unidad
- Expansión de la capacidad en línea (OCE)
- Tamaño de banda configurable de hasta 1 MB
- Hot Spare global y dedicado con Hot revertible
- Borrado seguro instantáneo
- Migrar el tamaño de RAID / Stripe
- Modificación de la política de escritura en caché
- Mover unidad lógica

O

- Vuelva a habilitar la unidad lógica fallida o Controlador RAID x32 basado en PCIe con caché de escritura respaldada por Flash de 8 GB, compatible con RAID 0, 1, 5, 6, 10, 50, 60, 1T, 10T que admite hasta 32 dispositivos de almacenamiento de conexión directa (SAS/SATA/NVMe). Debe admitir unidades SAS, SATA y NVMe combinadas en la misma controladora. El controlador debe ser compatible con 6G SATA, 24G SAS, 16G NVMe.

El controlador debe admitir lo siguiente:

- Expandir unidad lógica
- Borrado seguro instantáneo
- Migrar el tamaño de RAID / Stripe
- Modificación de la política de escritura de caché
- Mover unidad lógica
- Vuelva a habilitar la unidad lógica fallida

Networking features:

El servidor debe admitir las siguientes tarjetas de red:

- Adaptadores de red de 4 puertos de 1 Gb
- Adaptador Ethernet de 10 Gb y 2 puertos
- Adaptador Ethernet de 2 puertos 10GBaseT
- Adaptador Ethernet SFP28 de 2 puertos de 10/25 Gb
- Adaptador Ethernet SFP28 de 4 puertos de 10/25 Gb
- Ethernet QSFP28 de 2 puertos de 100 Gb
- Ethernet QSFP56 de 100 Gb y 1 puerto
- Ethernet QSFP56 de 2 puertos de 100 Gb
- Ethernet QSFP56 de 200 Gb

Opciones de Infiniband:

- Adaptador de puerto único o doble de 100 Gb o 200 Gb

Power Supply: Debe admitir fuentes de alimentación redundantes con bajo contenido de halógenos con una eficiencia mínima del 94%

Fans: Ventiladores redundantes del sistema de conexión en caliente

Industry Standard Compliance:

- Cumple con ACPI 6.4
- Compatible con PCIe 5.0
- Soporte WOL
- Certificaciones de logotipos de Microsoft®
- Soporte PXE

- Estrella de energía
- SMBIOS 3.4
- UEFI 2.7
- Redfish API
- IPMI 2.0
- Secure Digital 4.0
- Estándar de cifrado avanzado (AES)
- Estándar de cifrado de datos triple (3DES)
- SNMP v3
- TLS 1.2
- Arquitectura de gestión de sistemas DMTF para el protocolo de línea de comandos de hardware de servidor (SMASH CLP)
- Active Directory v1.0
- ASHRAE A3/A4

System Security:

- Compatibilidad con arranque seguro UEFI e inicio seguro
- Raíz de confianza de silicio inmutable
- Validación FIPS 140-2
- Certificación Common Criteria
- Configurable para el cumplimiento de PCI DSS
- Estándar de cifrado avanzado (AES) y estándar de cifrado de datos triple (3DES) en el navegador
- Soporte para algoritmos comerciales de seguridad nacional (CNSA)
- Tarjeta inteligente (PIV/CAC) y autenticación de 2 factores basada en Kerberos
- Actualizaciones sin manipulaciones: componentes firmados y verificados digitalmente
- Recuperación segura: recupere el firmware crítico a un buen estado conocido al detectar firmware comprometido
- Capacidad para revertir el firmware
- Borrado seguro de datos NAND/Usuario
- TPM (Módulo de plataforma segura) 2.0
- Opción de kit de bloqueo de bisel
- Opción de detección de intrusos en chasis

Operating Systems and Virtualization Software Support:

- Servidor de Windows.
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)
- VMware ESXi.
- Ubuntu canónico
- Oracle Linux y Oracle VM
- Citrix

Provisioning:

- Debe admitir una herramienta para aprovisionar el servidor mediante la API RESTful para descubrir e implementar servidores a escala
- Aprovisione de uno a varios servidores mediante scripts propios para detectar e implementar con Scripting Tool (STK) para Windows y Linux o Scripting Tools para Windows PowerShell

Firmware security:

- Para la seguridad del firmware, el sistema debe admitir un chip de administración remota que cree una huella digital en el silicio, evitando que los servidores se inicien a menos que el firmware coincida con la huella digital. Esta característica debe ser inmutable
- Debe mantener un repositorio de recetas de firmware y controladores para ayudar a revertir o parchear el firmware comprometido. También debe almacenar la receta de recuperación de fábrica precargada para revertir al firmware seguro probado de fábrica

Embedded Remote Management and firmware security:

- La administración remota del sistema debe admitir la consola remota gráfica basada en navegador junto con el botón de encendido virtual, el arranque remoto mediante una unidad USB / CD / DVD. Debe ser capaz de ofrecer la actualización de software y parches desde un cliente remoto utilizando Media/image/folder; Debe admitir la limitación de energía del servidor y los informes históricos y debe tener soporte para la autenticación multifactor
- El servidor debe tener un puerto de administración remota dedicado de 1 Gbps

- El servidor debe tener espacio de almacenamiento destinado a ser utilizado como repositorio para firmware, controladores y componentes de software. Los componentes se pueden organizar en conjuntos de instalación y se pueden usar para revertir / parchear firmware defectuoso
- El servidor debe admitir la administración sin agente mediante el puerto de administración remota fuera de banda
- El servidor debe admitir el monitoreo y el registro de cambios en el hardware del servidor y la configuración del sistema.
- Autenticación de dos factores
- Consola remota que comparte hasta 6 usuarios simultáneamente durante la operación previa al sistema operativo y al tiempo de ejecución del sistema operativo, reproducción de la consola. Integración de Microsoft Terminal Services, cifrado SSL de 128 bits y compatibilidad con Secure Shell versión 2. Debe proporcionar funcionalidad de actualización remota de firmware.
- Debe admitir la administración de varios servidores como uno solo a través de
    - Control de potencia de grupo
    - Límite de energía de grupo
    - Actualización de firmware de grupo
    - Configuración de grupo
    - Medios virtuales de grupo y medios virtuales cifrados
    - Activación de licencias grupales
- Debe admitir la integración de la API RESTful
- El sistema debe admitir soporte remoto integrado para transmitir eventos de hardware directamente al OEM o a un socio autorizado para soporte telefónico
- El servidor debe tener un panel de seguridad: muestra el estado de las funciones de seguridad importantes, el estado de seguridad general del sistema y la configuración actual de las funciones de bloqueo de configuración del servidor y estado de seguridad.
- Pantalla de nivel de desgaste NVMe
- Asesor de rendimiento de carga de trabajo: proporciona recomendaciones de ajuste del servidor para mejorar el rendimiento del servidor

10. ESPECIFICACIONES LIBRERÍA DE BACKUP:

Capacidad:

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- La biblioteca de cintas ofrecida admitirá una capacidad de datos nativa de 5 PB (sin comprimir) utilizando la tecnología LTO-9.
- Se ofrecerá con un mínimo de tres unidades de cinta LTO-9 FC. La unidad debe admitir el cifrado
- Se ofrecerá con 40 ranuras para cartuchos y será escalable a 280 ranuras.

Arquitectura de la unidad de cinta:

- La unidad LTO-9 ofrecida en la biblioteca debe cumplir con la técnica de coincidencia de velocidad de datos para una mayor confiabilidad
- La arquitectura de la unidad de cinta en la biblioteca debe cumplir con el protocolo ADI estándar INCITS T10 o estándares más recientes.

Escalabilidad: La biblioteca de cintas debe ser escalable a un número mínimo de 21 unidades LTO-9.

Velocidad: La unidad LTO-9 ofrecida debe admitir 300 MB / seg en modo nativo.

Conectividad: La biblioteca de cintas ofrecida proporcionará conectividad FC nativa a los conmutadores SAN.

Particionado: La biblioteca de cintas ofrecida debe tener flexibilidad para configurar cada unidad ofrecida en una partición separada. La biblioteca de cinta ofrecida tendrá soporte para 21 particiones cuando esté completamente llena.

Dispositivo de cifrado: La Biblioteca ofrecida se proporcionará con un dispositivo de hardware como una llave USB, un dispositivo separado, etc. para mantener todas las claves cifradas de manera redundante.

Administración: La biblioteca de cintas proporcionará administración remota basada en la web.

Lector de código de barras y ranuras para correo:

- La biblioteca de cintas debe ser compatible con el lector de códigos de barras y la ranura de correo.
- La biblioteca de cintas se ofrecerá con 5 ranuras de correo y será escalable a 30 ranuras cuando esté completamente poblada.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Otras características:

- La biblioteca de cintas debe tener un panel de interfaz gráfica de usuario
- Se puede montar en bastidor.
- Tendrá opción de fuente de alimentación redundante
- La biblioteca de cintas se suministrará con un software que pueda predecir y prevenir fallas a través de una alerta temprana y también sugerirá la acción de servicio requerida.
- Las unidades ofrecidas en la biblioteca de cintas admitirán opcionalmente la conmutación por error de la ruta de datos y la ruta de control.
- El software ofrecido también tendrá la capacidad de determinar cuándo retirar los cartuchos de cinta y qué relación de compresión se está logrando.

11. ESPECIFICACIONES SW´s:

Arquitectura: Switch ToR de 1 RU, L2/L3.

INTERFACES

Puertos para datos:

- 48x puertos 10G Base-T
- 6x puertos QSFP+

Todas las interfaces deben estar habilitadas, activas y listas para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.

Puertos para administración:

- 1 puerto serial de consola RJ45
- 1 puerto de consola mini USB
- 1 puerto de administración RJ45
- 1 puerto de administración SFP
- 1 USB para administración de archivos

CARACTERÍSTICAS GENERALES Y PERFORMANCE

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Características de memoria

- 4 GB RAM, 1 GB Flash, Packet buffer: 12 MB

Rendimiento:

- Switching 1440 Gbps
- Throughput 1071 Mpps
- Arquitectura nonblocking

Sistema Operativo:

El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio mencionados en esta ficha. Los servicios especiales que requieran licenciamiento avanzado se deben mencionar expresamente.

REQUERIMIENTOS L2

Tamaño de tablas: 208000 direcciones MAC

VLANs: 4094 VLAN

Tramas: Jumbo frames de hasta 10K bytes

Spanning tree:

- Spanning tree estándar IEEE 802.1D
- Rapid STP IEEE 802.1w
- Multiple STP (MSTP) IEEE 802.1s

Características:

- VXLAN
- ERPS (Ethernet Ring Protection Switching)
- Ethernet Link aggregation, soporte de hasta 1024 grupos
- IGMP
- LLDP

REQUERIMIENTOS L3

Performance:

- 16000 rutas IPv4
- 8000 rutas IPv6

Protocolos:

- ECMP
- Rutas estáticas IPv4/IPv6
- RIP, RIPng
- OSPF, OSPFv2, OSPFv3
- BGP-4, MP-BGP-4
- Dual Stack IPv4/IPv6

Características:

- ARP: estático, dinámico, proxy ARP
- DNS: cliente
- DHCP: relay, server, cliente

MULTICAST

Multicast Listener Discovery: MLD para IPv6, v1 y v2

Protocol Independent Multicast (PIM):

- IGMP Snooping
- PIM SM (Sparse Mode)
- PIM para IPv6

Internet Group Management (IGMP): IGMP v1, v2 y v3

QoS

Encolamiento: Al menos:

- Strict Priority
- WRR

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570
Great Place To Work. Certificada
Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- DCB (Data Center Bridging), DCB Exchange protocol, Priority Flow Control (PFC), Enhanced Transmission Service (ETS)

Servicio: Al menos:
- 802.1p
- DSCP
- CoS

SEGURIDAD

Autenticación para administración: Soporte de:
- Radius
- TACACS+

Gestión segura: Acceso seguro a la gestión cifrando el tráfico (CLI, MIB) por medio de SSHv2, SNMPv3

Características: Al menos:
- Listas de acceso de control (ACL). También protegen el plano de control SSH, SNMP o NTP.
- Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador
- DHCP snooping, ayuda evitar problemas causados por servidores DHCP no autorizados
- DLDP.

Alta disponibilidad: Al menos:
- Ethernet Link aggregation
- Permitir una arquitectura distribuida y redundante mediante la implementación de dos switches y cada switch mantiene un control independiente, pero permanece sincronizado durante las actualizaciones o fallas. También admite actualizaciones durante la operación en vivo.
- BFD (Bidirectional Forward Detection)
- VRRP (Virtual Router Redundancy Protocol)
- Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario.

GESTIÓN

Administración:

- Capacidad de administración CLI
- CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores
- sFlow (RFC 3176)
- Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con protección por contraseña, registro de acceso local y remoto por syslog.
- TACACS+ proporciona autorización de acceso administrativo
- SNMP (v2c/v3) , MIBs estándar y extensiones privadas
- TFTP, SSH
- NTP
- Almacenamiento de múltiples archivos de configuración en memoria flash
- Port mirroring para tráfico saliente y entrante hacia puerto de monitoreo local o remoto.

HARDWARE Y ENERGÍA

Montaje: Debe traer todos los accesorios para montaje y operación en rack estándar de 19"

Alimentación eléctrica: Soporte al menos:

- AC 100-240 VAC.
- 50/60 Hz.

Redundancia en fuente de poder: 2 fuentes reemplazables en caliente.

Redundancia en ventilación: 5 arreglos de ventiladores reemplazables en caliente.

Medio ambiente: Cumplir al menos con RoHS

Temperatura de operación: 0°C a 45°C

Humedad de operación: 10% a 90% no condensada

12. EVALUACIÓN DE LA SOLUCIÓN OFERTADA:

Los proponentes deberán anexar a su oferta las fichas técnicas de los equipos ofertados, el licenciamiento de virtualización y Sistema Operativo.

ENTIDAD CERTIFICADA
CO-SC-CER303297 ST-CER655785 CO-SI-CER1017570

Secretaría TIC
Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Central Piso 7.
Código Postal: 111321 – Teléfono: 749 1513
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Los oferentes deberán diligenciar los anexos:

- ANEXO 10: ESPECIFICACIONES NODOS DE HYPERCONVERGENCIA
- ANEXO 10.1 ESPECIFICACIONES SERVIDOR DE BACKUP
- ANEXO 10,2 ESPECIFICACIONES LIBRERÍA DE BACKUP
- ANEXO 10.3. ESPECIFICACIONES SW´s

Indicando si cumplen o no cumplen y citando la página de la ficha técnica donde se puede evidenciar el cumplimiento de los criterios técnicos definidos por la Entidad.