Gobernación de Cundinamarca

ANEXO 10: ESPECIFICACIONES NODOS DE HYPERCONVERGENCIA				
Marca y Modelo (por favor especificar):		**CUMPLE**		**Pág ficha tecnica**
ITEM	**DESCRIPCION**	**SI**	**NO**	
1	**Infraestructura hiperconvergente:** 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.			
2	**REQUISITOS DE HARDWARE Y RENDIMIENTO**			
2.1	**Especificaciones de hardware:** •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. •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.			
2.2	**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.			
2.3	**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. •La deduplicación y la compresión se realizarán en línea, independientemente del tipo de E/S, como operaciones secuenciales o aleatorias.			
2.4	**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.			

2.5	**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.			
2.6	**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.			
3	**REQUISITOS DE SOFTWARE Y FUNCIONALIDAD**			
3.1	**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.			

3.2	**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. •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.			
3.3	**Habilitado para la nube: monitoreo, inteligencia artificial e integración de hipervisor:** •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.			

3.4	**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.			
3.5	**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.			
3.6	**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			

3.7	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. •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.			
3.8	**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			
3.9	**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.			

3.10	**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 in •Licenciamiento SO: Microsoft Windows Server 2025 Datacenter para la totalidad de los cores por 5 años • VMware vSphere Foundation o su sustituto última versión 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.			