

Anexo 1 - FICHA TÉCNICA

1. ITEM: SOLUCIÓN DE HIPERCONVERGENCIA	
Denominación Técnica:	Solución de Hiperconvergencia HCI
Clasificación UNSPSC:	43201800 Dispositivos de almacenamiento 43211500 Computadores 43212200 Sistemas de manejo de almacenamiento de datos de computador 43222600 Equipo de servicio de red 43232800 Software de administración de redes 43233000 Software de entorno operativo 43233700 Software de administración de sistemas 72103302 Mantenimiento o soporte de equipo de telecomunicaciones 80101500 Servicios de consultoría de negocios y administración corporativa 81111500 Ingeniería de software o hardware 81111700 Sistemas de manejo de información MIS 81111800 Servicios de sistemas y administración de componentes de sistemas 81111900 Sistemas de recuperación de información 81112000 Servicios de datos 81112200 Mantenimiento y soporte de software 81112300 Mantenimiento y soporte de hardware de computador 86101700 Servicios de capacitación vocacional no - científica
Unidad de Medida:	Unidad
CONDICIONES GENERALES	
GENERALIDADES	El Ministerio del Deporte requiere adquirir una solución de hiperconvergencia que le ofrezca computación, almacenamiento, redes y software de virtualización en un entorno unificado que permita a la entidad optimizar y simplificar la gestión y administración de la plataforma tecnológica propia.
	Igualmente, requiere poder crecer de forma granular mediante la adición de nodos completamente integrables según lo requiera la entidad; la inclusión o integración de una librería de cintas LTO para copias de respaldo de información, de archivado y de recuperación ante desastres, y que la solución ofrecida optimice la eficiencia del consumo y uso del almacenamiento disponible garantizando una correcta y eficiente operación.
	Todos los componentes de la solución ofertada deben ser nuevos de fábrica, sin ninguna pieza remanufacturada, ni reparada.
	El proponente deberá incluir los catálogos o manuales o URL propia del fabricante de hiperconvergencia para soportar técnicamente cada uno de los elementos de la propuesta, junto con la presentación de la oferta.
	El soporte para todo el hardware debe ser de 3 años.
	El soporte para todo el software debe ser de 3 años

Anexo 1 - FICHA TÉCNICA

	El fabricante deberá disponer de una organización formal de soporte empresarial para Latinoamérica, con atención 7x24x365, procedimientos oficiales de escalamiento a ingeniería de producto y disponibilidad de atención en idioma español. El soporte solicitado tanto en hardware como en software deberá estar alineado con los tiempos y el nivel de servicio descrito en el ítem 5 Servicios profesionales para el despliegue de la solución, en cuyo caso el oferente ganador del proceso hará la intermediación entre el Ministerio y los fabricantes.
1	CARACTERÍSTICAS TÉCNICAS SOLUCIÓN DE HIPERCONVERGENCIA
1.1.	Cantidad de nodos: La solución debe estar compuesta por mínimo 3 Nodos o Appliances de procesamiento para la hiperconvergencia, los cuales deben ser certificados por el fabricante, distribuidos como se indica en los numerales 1.2, 1.3, 1.4, 1.5 y 1.6.
1.2.	Procesadores por nodo: • Mínimo dos (2) procesadores de 3.2 GHz o superior por nodo/appliance. • Solo se consideran propuestas con procesadores mínimo de quinta generación • Arquitectura de 16 cores mínimo por servidor. • El software de gestión de hiperconvergencia a adquirir debe poder implementarse sobre nodos con procesadores Intel o AMD.
1.3.	Características generales: • Dos (2) fuentes de poder de 110v – 240v AC redundantes por nodo • Montaje Rackeable. • El espacio requerido en rack por cada nodo o Appliance de hiperconvergencia ofertado no debe superar dos (2) unidades de rack (2U). • Deben incluirse todos los elementos necesarios para instalación en Rack como rieles, herrajes, cables de poder, etc.
1.4.	Memoria RAM: • Cada nodo debe contar como mínimo con 1024 GB de memoria RAM y con slots libres suficientes para duplicar esta capacidad • DDR5 a 5600-MHz como mínimo
1.5.	Conectividad: • Compatible con IPv4 e IPv6. • Una (1) tarjeta de dos (2) Puertos 10/25Gb por nodo de hiperconvergencia, incluyendo los conectores (Transceivers) SFP y fibras para conectar la solución. • Dos (2) puertos 10 GbE RJ45 por nodo (ya sea integrados en la tarjeta principal o por medio de una tarjeta de expansión). • Cada nodo deberá contar con una interfaz o mecanismo de conexión dedicada para la administración remota fuera de banda (OOBM) de la solución con el máximo

Anexo 1 - FICHA TÉCNICA

	licenciamiento disponible, de acuerdo con la arquitectura del fabricante de la solución. • Debe incluir cables (poder, red, fibra óptica, entre otros), rieles de montaje y demás elementos requeridos para su instalación y puesta en funcionamiento.
1.6.	Almacenamiento: • Se debe garantizar una capacidad de almacenamiento efectiva utilizable mayor o igual a 69 TB, inclusive luego de la caída de un nodo de la solución. Para el cumplimiento de este requisito, se aceptará una eficiencia mínima de almacenamiento de 1.5:1 derivada de mecanismos de deduplicación y compresión, con el fin de optimizar los costos de la solución. • La solución deberá garantizar una capa de almacenamiento en estado sólido (SSD). Los discos de la solución deberán contar con una capacidad mínima de 3.84 TB cada uno, manteniendo las características de disponibilidad y resiliencia requeridas para minimizar la ventana de indisponibilidad. • La solución de hiperconvergencia deberá integrar funcionalidades de compresión y deduplicación de acuerdo con la arquitectura técnica de cada fabricante, aplicadas eficientemente sobre el total de capacidad ofertado (grupo de discos, nodo o globalmente, según la arquitectura del fabricante). La plataforma deberá implementar una arquitectura de almacenamiento All Flash basada exclusivamente en unidades SSD y/o NVMe, de acuerdo con las mejores prácticas y lineamientos del fabricante. No se aceptarán discos HDD ni configuraciones híbridas de almacenamiento. • Para efectos de la propuesta, ninguno de los componentes contenidos en la solución podrá estar en listas de fin vida o fin de soporte de los fabricantes, en los próximos 3 años. • El almacenamiento ofrecido debe tener la capacidad de soportar fallo de mínimo un Nodo en toda la solución hiperconvergente sin pérdida de acceso o integridad de los datos. • No se aceptarán soluciones o configuraciones que manejen mecanismos de SAN tradicionales tipo FiberChannel como LUNs, volúmenes, grupos de discos o switches SAN dedicados para aprovisionar el almacenamiento de la solución hiperconvergente implementados mediante equipos físicos; no se excluye ofertar soluciones basadas en arquitecturas modernas de HCI desagregada, según las técnicas de solución que ofrezca cada fabricante. • El fabricante debe proveer licenciamiento total para funcionalidades críticas como snapshots, snapshots administrados desde aplicación, clones, replicación, QoS, entre otras funcionalidades, para toda la capacidad ofrecida.
1.7.	Operatividad: • El contratista deberá hacer entrega de la infraestructura mínima y necesaria para el correcto funcionamiento de la solución ofertada. Esta deberá ser instalada y configurada por parte del Contratista y verificada por parte de Mindeporte en las

Anexo 1 - FICHA TÉCNICA

	instalaciones de la entidad ubicadas en la Av 68 No 55-65, o en el Datacenter donde se encuentren alojados los equipos de la entidad en la ciudad de Bogotá. Con la presentación de la oferta El Contratista debe entregar certificación del fabricante en donde se confirma el servicio de implementación de la solución ofertada en los términos requeridos por el Ministerio del Deporte. • La solución ofertada debe incluir el software de hipervisor que permita la creación del ambiente virtual de la entidad. Este debe incluir el soporte y actualizaciones a nuevas versiones sin costo adicional durante el periodo de garantía. • El contratista deberá certificar mediante carta emitida por el fabricante que la garantía, soporte y mantenimiento por parte del fabricante es de tres (3) años. • La solución debe incluir 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, el cluster se mantenga operativo sin afectar la operación de las aplicaciones, según las técnicas de solución que ofrezca cada fabricante. • La solución de hiperconvergencia debe estar en capacidad de soportar servidores de archivos y almacenamiento según las técnicas de solución de cada fabricante. • Los nodos a ofrecer para conformar el clúster deben estar certificados, pre-testeados y precargados en fábrica para funcionar de forma correcta con el software de hiperconvergencia entregando un único punto de contacto de soporte. • La solución ofrecida deberá tener la capacidad de fallo de como mínimo uno de los nodos o Appliance, (basado en la premisa que no se cuente con un disco, o este reportado como dañado o degradado sobre la solución) sin pérdida de acceso o integridad de los datos.
1.8.	Características del software de gestión de hipervisor / hiperconvergencia: • La consola de administración de la solución ofrecida deberá entregar estadísticas completas de consumos de CPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias. • La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, firmware de los nodos, versión de BIOS e hipervisor) de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni indisponibilidad del servicio. • La solución también debe soportar integración mediante el uso de REST API, con el fin de vincularla a otra solución de administración para facilitar la integración con ambientes de monitoreo actuales. • La solución debe proveer un mecanismo para ingresar un nodo en modo de mantenimiento, modo en el que se debe preservar la disponibilidad de los datos. Este comportamiento se debe mantener en las configuraciones de clúster ofertadas. • La solución debe incluir una funcionalidad automática que periódicamente haga una revisión al estado de salud de todos los componentes tanto de hardware como de software del clúster y entregue un reporte detallado para la resolución de problemas.

Anexo 1 - FICHA TÉCNICA

	- La solución debe incorporar una tecnología estándar en la industria para ejecutar chequeos de integridad de los datos. - La solución debe proveer un esquema de alta disponibilidad para la capa de administración de la infraestructura hiperconvergente, de manera que la falla de un nodo o del componente de gestión no impida la operación ni la administración del clúster. El esquema provisto podrá estar embebido de forma nativa en la arquitectura del fabricante o habilitarse mediante configuración según sus mejores prácticas. - La solución debe incluir una funcionalidad que notifique automáticamente al fabricante acerca de condiciones de error de manera proactiva. - La solución debe incluir una funcionalidad según las técnicas de solución de cada fabricante que permita realizar proyecciones de capacidad y tareas de planeación. - La solución debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas, ya sea directamente desde la solución de hiperconvergencia o desde el hipervisor. - La solución debe tener la capacidad de monitorear el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales, en lugar de esperar a que las condiciones estén violando alguna regla, política o umbral. Esta funcionalidad se realizará de acuerdo con el método de cada fabricante. - La solución debe incluir una función que permita a la entidad crear tareas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración o según las técnicas de solución de cada fabricante.
1.9.	Requerimientos generales de la solución a ofertar: - Debe ofrecer el servicio para el manejo de imágenes y/o plantillas de máquinas virtuales disponibles para el hipervisor. - Debe permitir la adición en caliente de recursos de memoria y capacidad de almacenamiento a una máquina virtual. - Debe incluir un portal web o software de autogestión de aprovisionamiento de recursos de cómputo y almacenamiento que permita la asignación de recursos a áreas de producción, desarrollo o pruebas con la capacidad de creación de catálogos o plantillas de máquinas virtuales. Debe soportar autenticación en este portal mediante el directorio activo. - Debe poder ser actualizado desde la misma consola de gestión del sistema hiperconvergente o desde el hipervisor a las últimas versiones sin interrupción del servicio. - Debe incluir las herramientas necesarias para ver todas las estadísticas funcionales y operacionales del clúster a nivel de máquina virtual. - Debe soportar la compatibilidad automática entre diferentes generaciones de CPUs del mismo fabricante.

Anexo 1 - FICHA TÉCNICA

	• La solución ofrecida debe ser basada en un software agnóstico capaz de desplegarse sobre diversas arquitecturas e independiente del fabricante de los procesadores. • La solución de hiperconvergencia ofertada deberá incluir el licenciamiento necesario para cubrir todo el hardware incluido en la oferta según los requerimientos en este documento y la posibilidad de recibir actualizaciones y parches sin costo adicional durante la vigencia del licenciamiento • Debe contar con todo el licenciamiento que permita administrar los recursos físicos (Memoria, procesador, almacenamiento) actuales. • Debe contar con el licenciamiento necesario para habilitar un esquema en alta disponibilidad sobre las máquinas virtuales de forma nativa y autónoma. • El sistema hiperconvergente debe llevar a cabo las actividades de compresión y deduplicación completamente en software. • La solución requerida debe incorporar la capa de software de administración de la infraestructura de hiperconvergencia como un servicio, instalada en cada uno de los nodos o appliance que componen la solución, manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información. • La solución debe incluir un sistema de gestión global y federada que permita integrar los diferentes nodos en una sola interfaz, garantizando compatibilidad de despliegue, y que permita la gestión total sobre los recursos, máquinas virtuales (almacenamiento, procesamiento y memoria RAM), rutinas de mantenimiento incluyendo export e import de instancias, mecanismos de Failover para balancear las cargas entre nodos, y migración manual o automática de VM's hacia el siguiente nodo en caso de falla. • El hipervisor ofrecido con la solución de hiperconvergencia, debe incluir la funcionalidad de ubicación inteligente de máquinas virtuales utilizando estadísticas de uso de CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las cargas de trabajo el mejor acceso posible a los recursos. Esta funcionalidad debe venir habilitada por defecto. • El hipervisor ofrecido con la solución de hiperconvergencia, debe permitir la definición de redes virtuales por software (SDN) mediante un switch virtual con soporte y mapeo de vLANs, Link Aggregation, y visualización sobre los puertos físicos del switch TOR (Top Of Rack). • La solución ofrecida deberá ser capaz de crecer en número de nodos o appliance bajo el esquema de alta disponibilidad descrito en este documento, según las mejores prácticas del fabricante y con características técnicas iguales o superiores a las mencionadas en este documento, lo cual se deberá soportar por medio de una certificación del fabricante directamente donde se confirme la validez de este punto. • El soporte técnico y actualizaciones descrito en este ítem se deberá proyectar para un periodo de vigencia no inferior a 3 años. • El licenciamiento deberá quedar a nombre del Ministerio del Deporte.
--	---

Anexo 1 - FICHA TÉCNICA

	• Con el fin de validar y comprobar las diferentes funcionalidades ofrecidas, el proponente deberá adjuntar documentación propia del fabricante como catálogos, manuales o enlaces de internet, que soporten cada una de las respuestas del presente proceso. • La solución deberá encontrarse certificada y soportada oficialmente para operar sobre al menos dos (2) plataformas de nube pública catalogadas como líderes del mercado por firmas internacionales de consultoría y análisis tecnológico, permitiendo la movilidad de cargas de trabajo y una administración consistente entre los ambientes locales y la nube • El licenciamiento ofertado deberá corresponder a un esquema empresarial vigente del fabricante, administrable por la entidad y con capacidad de movilidad entre ambientes on-premise y nube híbrida oficialmente soportados por el fabricante. La continuidad del soporte, actualizaciones y renovación deberá estar garantizada durante toda la vigencia contractual • La solución debe soportar el despliegue y ejecución de aplicaciones basadas en contenedores y arquitecturas de microservicios mediante plataformas de orquestación tipo Kubernetes, ya sea integradas o con conformidad certificada por la CNCF para operar sobre la infraestructura HCI ofertada. La integración deberá estar soportada oficialmente por el fabricante y permitir la administración centralizada de los recursos de cómputo, almacenamiento y contenedores. • La solución deberá incorporar funcionalidades avanzadas de virtualización y segmentación de red, incluyendo microsegmentación, aislamiento de cargas de trabajo y dominios de red independientes, de forma nativa o mediante componentes oficialmente soportados por el fabricante. Dichas capacidades deberán contar con soporte empresarial y disponibilidad de soporte especializado en Colombia y Latinoamérica. • La solución debe tener la capacidad de aprender el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales, en lugar de esperar a que las condiciones estén violando alguna regla, política o umbral. • Dado que la entidad busca garantizar una inversión inicial eficiente, y con el fin de asegurar que los crecimientos futuros de la solución se adapten a las necesidades específicas, la solución deberá permitir la expansión del clúster mediante la incorporación de nuevos nodos y generaciones de hardware, siempre que dicha combinación se encuentre formalmente certificada, documentada y soportada por el fabricante dentro de sus matrices oficiales de compatibilidad (incluyendo nodos en configuración All Flash o híbrido en el mismo clúster). Se deben asegurar todas las funciones descritas en el presente documento para clústeres configurados bajo esta premisa.
--	--

Anexo 1 - FICHA TÉCNICA

	- La funcionalidad de compresión ofrecida debe ejecutarse tanto en línea como posterior al almacenamiento del dato. La entidad requiere que este proceso se pueda activar o no, con el fin de asegurar el mejor desempeño y ajustarse a las recomendaciones y/o requerimientos de los diferentes proveedores o fabricantes. - La solución debe contar con mecanismos simplificados para el despliegue del servicio de archivos, (wizard de configuración) operados y gestionados desde la misma plataforma de administración de la solución, de conformidad con la solución técnica de cada fabricante. - La solución debe incluir técnicas de optimización del almacenamiento diferentes a compresión y/o deduplicación (Ej., thin provisioning, erasure coding (RAID-5/6) o similares, acorde con la arquitectura de cada fabricante). - La solución debe permitir la exportación de almacenamiento en forma de bloques a servidores externos mediante el protocolo iSCSI o NFS, sin requerir que los servidores estén alojados dentro de la solución de virtualización - La solución deberá implementar mecanismos distribuidos de protección de datos y resiliencia certificados por el fabricante, permitiendo configurar diferentes niveles de protección para las cargas de trabajo y garantizando la continuidad operativa ante la falla total de al menos un nodo del clúster, sin pérdida de disponibilidad o integridad de la información. - El proponente deberá ser canal autorizado del fabricante de la solución ofertada y contar con personal técnico certificado vigente en las tecnologías ofrecidas. El fabricante deberá disponer de un programa formal de certificación técnica y especialización para sus socios de negocio, así como de una red de canales autorizados con capacidad de prestación de servicios en Colombia.
1.10	Conectividad de la solución a la actual red LAN de la entidad: - La entidad cuenta con 2 switches Core grado empresarial marca Cisco, familia Catalyst 9500, referencia C9500-48Y4C-A, con puertos disponibles, que se planea utilizar para conectar los elementos de la solución a adquirir a la red interna, con separación por VLANs, y ofreciendo alta disponibilidad. - Deben incluirse en la oferta presentada los módulos SFP+ 10Gigas, de acuerdo a la infraestructura ofertada y compatibles con los switches mencionados, en la cantidad requerida para permitir la conexión de los diferentes elementos a través de estos 2 switches existentes. - Deben también incluirse en la oferta los patchcord en la cantidad requerida para conectar los componentes de la solución ofertada a la LAN; se planea colocar los elementos de la solución a adquirir en un rack de 42U adyacente al rack donde ya están instalados los 2 switches Cisco, con una separación máxima de 5mts
1.11	Servicios conexos:

Anexo 1 - FICHA TÉCNICA

	- El oferente debe adjuntar carta del fabricante de la solución de hiperconvergencia donde certifique que es distribuidor autorizado para Colombia de los productos y/o servicios ofertados como partner mínimo en nivel medio o equivalente en la escala de cada fabricante es decir que puede ser Silver, profesional o equivalente de acuerdo con cada fabricante. La certificación no debe ser mayor a treinta (30) días anteriores a la fecha del cierre del actual proceso. - Los servicios de instalación y/o configuración podrán ser prestados directamente por el fabricante o por el oferente, mediante personal propio certificado por el fabricante en la solución ofertada. El oferente deberá demostrar dichas certificaciones mediante la documentación correspondiente, vigente a la fecha de presentación de la oferta. Las certificaciones o cartas de respaldo emitidas por el fabricante no deberán tener una antigüedad superior a treinta (30) días calendario respecto de la fecha de presentación de la oferta. - El oferente de la solución deberá acreditar presencia comercial directa o mediante representación autorizada permanente en Colombia durante al menos cinco (5) años anteriores a la fecha de presentación de la oferta. - El oferente deberá acreditar como mínimo tres (3) implementaciones de infraestructura hiperconvergente en producción, de características similares a las requeridas en el presente proceso, ejecutadas en entidades gubernamentales o empresas de gran tamaño en Colombia o Latinoamérica durante los últimos cinco (5) años.
2	ÍTEM 2: SOLUCIÓN DE BIBLIOTECA DE CINTAS LTO-9 Y SERVIDOR PARA BACKUP.
2.1	Solución de biblioteca de cintas LTO Capacidad - Se deberán incluir 20 cartuchos de cinta de tecnología LTO-9. Arquitectura de la unidad de cinta - La unidad LTO-9 ofrecida en la Biblioteca deberá cumplir con la técnica de coincidencia de velocidad de datos para una mayor confiabilidad. - La arquitectura de la unidad de cinta en la Biblioteca deberá cumplir con el protocolo ADI del estándar INCITS T10 o estándares posteriores. Velocidad y Escalabilidad - La unidad LTO-9 ofrecida admitirá 300 MB/seg en modo nativo. - La biblioteca de cintas será escalable al doble de unidades LTO-9. La actualización de las unidades se realizará sin necesidad de herramientas. Dispositivo de cifrado - La biblioteca ofrecida deberá estar provista de un dispositivo de hardware como

Anexo 1 - FICHA TÉCNICA

	una llave USB, un dispositivo separado, etc. para mantener todas las claves cifradas de forma redundante. Conectividad y Administración - La biblioteca de cintas ofrecida proporcionará conectividad SAS nativa de 12 Gbps directamente a los servidores de backup. - La biblioteca de cintas proporcionará gestión remota basada en web. Lector de código de barras y ranuras para correo - La biblioteca de cintas deberá admitir un lector de código de barras y una ranura de correo. Particionado - La biblioteca de cintas ofrecida proporcionará la funcionalidad para configurar cada unidad en una partición separada, cuando se escala a dos unidades LTO9. Otras características - La biblioteca de cintas deberá contar con un panel gráfico. - Deberá ser montable en rack. - La biblioteca de cintas deberá contar con software que permita predecir y prevenir fallos mediante alertas tempranas y que también sugiera las acciones de servicio necesarias. - El software ofrecido también deberá poder determinar cuándo retirar los cartuchos de cinta y qué relación de compresión se está logrando. Características generales del servidor para backup - Debe incluir soporte y garantía por mínimo 3 años. - Chasis de 1U como máximo - CPU: mínimo un (1) procesador arquitectura x86-64 con 8 cores como mínimo. - Memoria: DIMM de mínimo 32GB, usando DDR5 que opere mínimo a 5600 MT/s - Dos (2) discos de 480 GB SATA 6G Read Intensive SFF configurado en RAID 1 - El servidor debe admitir hasta tres ranuras PCI-Express 5.0 x16. - Dos ranuras PCIe 5.0 x8 o superiores adicionales - Conexión tipo SAS (para conexión con la librería) - 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 - 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 mínimo 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)
--	--

Anexo 1 - FICHA TÉCNICA

	• 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 • Volver a habilitar la unidad lógica fallida El servidor debe admitir las siguientes tarjetas de red: • Debe estar configurado con 1 tarjeta de 2 puertos a 10Gbps en cobre o fibra, • 1 tarjeta para conexión externa SAS. • Debe soportar hasta 5 USB en total. • Puerto de administración dedicado de 1 GbE Fuentes de alimentación • Debe admitir fuentes de alimentación redundantes con bajo contenido de halógenos con una eficiencia mínima del 94% • Debe estar configurado con 2 fuentes de alimentación de 1000W con certificación Energy Star. • Ventiladores Redundant hot-plug system fans Cumplimiento de los estándares de la industria • Energy Star • SMBIOS 3.4 • UEFI 2.7 • IPMI 2.0 • Secure Digital 4.0 • Advanced Encryption Standard (AES) • Seguridad del servidor UEFI Secure Boot and Secure Start support • Common Criteria certification • Capacidad para revertir el firmware • TPM (Trusted Platform Module) 2.0 • Opción de kit de bloqueo de bisel • Opción de detección de intrusos en chasis • Soporte de sistemas operativos y software de virtualización Windows Server. Aprovisionamiento • Debe admitir la herramienta para aprovisionar el servidor mediante la API RESTful para detectar e implementar servidores a escala. • Debe permitir aprovisionar uno o varios servidores mediante scripts propios para detectar e implementar con Scripting Tool (STK) para Windows y Linux o Scripting Tools para Windows PowerShell
--	--

Anexo 1 - FICHA TÉCNICA

	• 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 firmware y controladores para ayudar a revertir o parchear el firmware comprometido. También debe almacenar el código de recuperación de fábrica precargada para revertir al firmware seguro probado de fábrica • 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 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 • Debe admitir la integración de la API RESTful • 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 Estado de seguridad y Bloqueo de configuración del servidor. • Borrado seguro con un solo botón diseñado para retirar / reutilizar servidores
2.2	Rack de comunicaciones. • La entidad cuenta con el rack para el montaje de la solución.
2.3	PDU (Unidad de Distribución de Poder) • La entidad cuenta con el rack para el montaje de la solución
3	ITEM 3: SOFTWARE DE BACKUP PARA SOLUCIÓN A CINTA.
3.1	• Se deben cubrir mínimo 40 máquinas virtuales. • El licenciamiento del software de Backup debe ser por suscripción e incluir el soporte y las actualizaciones de todos los componentes de la solución. El tiempo de la suscripción es de mínimo tres (3) años. • El software de Backup debe estar ubicado como líder dentro del cuadrante mágico de Gartner para soluciones de software de copia de seguridad y recuperación empresarial, en al menos tres (3) de los últimos cinco (5) años. • La solución deber proporcionar una única consola con capacidades para procesos de respaldo sin agentes para ambientes virtuales Onpremises, replicación de máquinas virtuales onpremises, gestión y distribución de agentes para maquinas físicas

Anexo 1 - FICHA TÉCNICA

	• La solución debe proporcionar una copia de seguridad eficiente "incremental para siempre" (primera copia de seguridad completa y copias sólo incrementales posteriores) e incluir opciones de copias de seguridad completas y ad-hoc para cualquiera que sea la carga objetivo (VM Onpremises, NAS, Servidor Físico) • La solución debe monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia si la latencia del datastore supera un umbral definido. • La solución debe detectar automáticamente los snapshot's huérfanos generados por la solución de respaldos y ejecutar de manera automática un proceso que permita su consolidación de forma consistente. • La solución deberá permitir tomar respaldos de Snapshots generados por el almacenamiento de producción de la entidad actualmente • La solución debe permitir la recuperación de Máquinas virtuales, archivos granulares de sistema operativo y de aplicación desde los snapshot's generados por el almacenamiento de producción • La solución deberá permitir la creación de Backup full sintéticos para máquinas virtuales de los ambientes virtuales sin importar el sistema operativo de la máquina objetivo (Linux - Windows) • La solución no debe requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la ejecución de tareas de recuperación granular de aplicaciones • En los procesos de respaldo se debe permitir truncar los registros de transacciones o archivos, sin el uso de agentes en las máquinas virtuales en ningún momento del proceso. • Los respaldos sin agente de máquinas virtuales deben proporcionar respaldo de logs o archivos de transacciones de los diferentes fabricantes de bases de bases, junto con copias de seguridad basadas en snapshots. • La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube. • La solución debe respaldar de forma consistente aplicaciones de base de datos MySQL y PostgreSQL que se ejecutan en Linux de forma consistente • La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo ejecutado por la solución y no debe depender de ninguna infraestructura de respaldo, por ejemplo, el catálogo central, para la recuperación. • La solución debe proporcionar tecnología de recuperación de respaldo de máquinas virtuales y máquinas físicas x86 de forma instantánea (encendido en menos de 5 minutos y automática) desde el repositorio de respaldos ya sea que se encuentren Onpremises o sobre un almacenamiento de Objetos en una nube pública • La solución debe poder utilizar la copia de seguridad o réplica de la máquina virtual para iniciar la máquina virtual en un entorno de red aislado para fines de prueba o certificación de respaldos
--	--

Anexo 1 - FICHA TÉCNICA

	• La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales, es decir, tener la capacidad de recuperar solo los bloques modificados desde el último respaldo y no la VM completa. • La solución debe permitir la recuperación de máquinas virtuales a través del canal de fibra SAN. • La solución debe poder escanear los datos de la máquina virtual a recuperar con un software antivirus antes de iniciar la restauración de la máquina al entorno de producción de forma integrada y automática. La solución debe abortar la operación de recuperación si se detecta malware. • La solución debe poder escanear los datos de respaldo de máquina virtual o agente a recuperar con un motor de búsqueda de firmas o patrones de malware totalmente personalizado de forma integrada y automática; esta funcionalidad debe permitir crear reglas para búsqueda de índices de compromiso personalizables. • La solución debe permitir la recuperación de archivos de sistema operativo directamente sobre una máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual. • La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web con la capacidad de buscar un archivo específico en todas las copias de seguridad. • La solución debe admitir la recuperación granular de bases de datos a partir de copias de seguridad basadas en imágenes • La solución debe proporcionar una interfaz de usuario de autoservicio basada en web con la capacidad de examinar y recuperar elementos de diferentes fabricantes de Bases de datos, • La solución debe permitir capacidades de Alta Disponibilidad (HA) donde se permitir la integración de varios repositorios de respaldos incluso de fabricantes diferentes en un solo repositorio virtual • La solución debe proporcionar un mecanismo fácil para expandir o adicionar el almacenamiento de respaldo de destino. • La solución debe admitir copias de seguridad deduplicadas y comprimidas en medios de cinta. • La solución debe admitir medios de cinta WORM. • La solución debe admitir de forma nativa el backup directamente y traslado de archivos de respaldo a almacenamiento de Objetos Azure, GCP y compatibles con protocolo S3. • La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube. • La solución debe proporcionar soporte para el almacenamiento de objetos Onpremises • La solución debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
--	---

Anexo 1 - FICHA TÉCNICA

	• La solución debe ofrecer inmutabilidad para el repositorio Onpremises de primer nivel y de almacenamiento de objetos de forma nativa • La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad, incluso ambas opciones deben poder habilitarse en una misma política. • La solución debe encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo. • La solución debe tener la capacidad de integrarse con SAML 2.0 para la autenticación extendida. • La solución debe hacer detección de malware en línea, realizando un análisis de entropía en línea y de bajo impacto para detectar de inmediato datos que anteriormente no estaban encriptados y que ahora están siendo cifrados por Ransomware, utilizando un modelo de Aprendizaje Automático (ML) especialmente entrenado. • La solución deberá realizar detección de actividad sospechosa en el sistema de archivos, con búsqueda en los índices del sistema de archivos con extensiones conocidas de malware, notas de rescate y señales similares de presencia de malware. • Deberá permitir la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma • La solución debe leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia. En caso de que se detecte corrupción de datos, la solución debe reconstruir automáticamente el bloque dañado con datos de producción. • La solución deberá poder programar tareas de encendido automático de las máquinas virtuales a partir de los respaldos y ejecutar tareas de verificación de sistema operativo y la disponibilidad de aplicaciones. Esta prueba no debe tener impacto en la red de producción. La solución debe proporcionar un informe de verificación de recuperación. • La solución debe tener la capacidad de escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo. • La solución deberá permitir prevenir la eliminación accidental o errónea de copias de seguridad o repositorios completos, cambios en usuarios, roles y otros ajustes de acceso mediante la consola de administración, requiriendo la aprobación de un segundo Administrador de la solución. • La solución debe presentar la tecnología de replicación directa de máquina virtuales sin depender de tareas de respaldo para lograr la replicación, igualmente debe implementar procesos de <i>failover</i> y <i>failback</i>. • Las copias de respaldo secundarias deberán ser independientes de la copia principal y podrán seleccionar diferentes puntos de retención con soporte a estrategias GFS
--	---

Anexo 1 - FICHA TÉCNICA

	• La solución debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de optimizar la utilización del ancho de banda. • La solución deberá permitir la integración de soluciones externas de tipo SIEM para correlación de eventos • La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas Onpremises y Cloud • La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo. • La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría. • La solución debe ofrecer un <i>dashboard</i> donde se evidencie la postura de seguridad de la plataforma de respaldo • La solución debe ofrecer la capacidad de generar alarmas y acciones de remediación en monitoreo de procesos de backup y gestión de la plataforma virtual • Se debe proveer la capacidad de generar reportes personalizados basados en datos de inventario y uso de recursos de la plataforma virtual, como también de la plataforma de respaldo • La solución debe proporcionar informes de cambios de configuración de la plataforma virtual y de respaldos con fines de auditoría. • La solución debe proporcionar informes de uso por cada uno de los almacenamientos usados por la solución, Onpremises o cloud • La solución debe proporcionar informes históricos y actuales de las sesiones de respaldo para todos los tipos de cargas configurados en la solución (Cloud - Onpremises) • La solución debe proporcionar informes tipo <i>chargeback</i> del uso de recursos • Deberá ofrecer un conjunto de reportes capaces de presentar la siguiente información: - Reportes que permitan la planificación de la capacidad - Reportes que permitan la determinación de ineffectividad en el uso de recursos. - Reportes que faciliten la visibilidad de tendencias negativas y anomalías de respaldo y uso de almacenamiento - Envío automático y programado de reportes de auditoría para operaciones de recuperación y modificaciones a políticas de respaldos o replicación - Tableros de control claros, presentables e integrables en sitios web" • La solución deberá integrar una solución de MFA para el acceso a la consola de gestión y administración • Los componentes de la solución de respaldo deben ser capaces de admitir autenticación Kerberos. • Se deberá tener soporte para IPv6
--	--

Anexo 1 - FICHA TÉCNICA

	- La solución podrá hacer recuperaciones de imagen sobre ambientes de nube pública como Azure, AWS y GCP - La solución deberá replicar de forma asíncrona máquinas virtuales sin <i>snapshots</i> del ambiente virtual y debe capturar todas las E/S de escritura directamente del disco de la VM, sin tener dependencia del hardware, sin limitación de distancia - La capacidad de replicación y respaldo debe estar incluida en la misma licencia - La solución debe permitir mover los respaldos entre las tareas y copiar los respaldos entre repositorios - La solución debe admitir de forma nativa la copia de respaldo a cinta sin requerir software adicional para su administración, permitiendo el uso de medios de cinta WORM - La solución deberá proveer la capacidad de implementar planes de recuperación (automatización de tareas) de las siguientes fuentes: Backup, Réplicas, Réplicas sin snapshots, Réplicas de storage - La solución deberá integrar capacidades de reportes personalizables de todas las actividades de cada plan de recuperación cada vez que se ejecute un plan de ejecución, pruebas, validación de prerrequisitos - Para los planes de recuperación (automatización de tareas) la solución deberá incluir pasos configurados por defecto y la capacidad de agregar pasos personalizables y que permitan la inclusión de scripts bajo Powershell - La solución de orquestación deberá incluir la capacidad de generar ambientes de pruebas de cada uno de los planes de recuperación para trabajos de Backup de VM y agentes, replica, replica sin snapshots. - La solución de orquestación debe incluir diferentes capacidades para validar que las recuperaciones no están comprometidas con malware.
4	ITEM 4: MEMORIAS RAM PARA ACTUALIZAR SERVIDORES HP PROLIANT
4.1	- La entidad cuenta con dos (2) servidores HPE ProLiant DL380 Gen11 (P60638-B21) con 128 GB de RAM cada uno y se requiere ampliarlos en RAM para poder alojar más máquinas virtuales, - Cada servidor cuenta con 4 módulos de 32 GB DDR5 EC8 RDIMM 2Rx8 PC5-4800B, P/N P48501-001, 2 módulos por CPU para un total de 4 módulos RDIMM por servidor. - Se requiere actualizar cada servidor a 384 GB en RAM mediante la adición de módulos de memoria compatibles atendiendo las reglas de poblado de memoria de la placa base de los servidores.
5	ITEM 5: INSTALACIÓN Y CONFIGURACIÓN DE LAS SOLUCIONES.
5.1	Se requiere cubrir totalmente la instalación, configuración y puesta a punto de la infraestructura tecnológica a adquirir, la migración de máquinas virtuales actuales y la conversión de los servidores físicos que determine el Ministerio, garantizado el funcionamiento de estos sobre la nueva plataforma de virtualización instalada.

Anexo 1 - FICHA TÉCNICA

	• Se debe garantizar que las maquinas físicas migradas tengan operatividad tras convertirlas a máquinas virtuales sobre el hipervisor ofrecido y en caso de presentarse alguna falla tras su conversión, el oferente deberá disponer de los recursos humanos y técnicos necesarios en aras de resolver los inconvenientes técnicos presentados. • Se deberá incluir transferencia de conocimiento en la administración y operación de la plataforma y se deberá entregar por escrito en físico o digital toda la documentación necesaria para actuar en caso de fallas en la solución, detallando qué elementos son susceptibles de reemplazar por el cliente y qué elementos requieren la intervención del personal de soporte del fabricante. • Realizar instalación física y configuración de los servidores de la plataforma de virtualización en los racks dispuestos por la entidad. • Realizar instalación física y configuración del servidor de backup. • Realizar instalación física y/o configuración de SFP's en los switches de la entidad • Realizar instalación física y configuración de la librería de backup. • Apoyar con la configuración en la integración entre la solución ofertada y los equipos de red existentes en Mindeporte. • Configurar el hipervisor adquirido. • Instalar y configurar la solución de backup. • Entregar la documentación técnica de la implementación en físico o digital • Realizar la configuración de las VLANs de la entidad a nivel del hipervisor. • Completar la lista de chequeo de pruebas técnicas de la plataforma, documentación que deberá ser coordinada entre las partes y aceptada por las mismas. • Efectuar la migración de las VM's actuales a la nueva plataforma. • Efectuar la conversión de servidores físicos a virtuales sobre la nueva plataforma. • En caso de que el personal que asigne el contratista no pueda desarrollar el objeto del proyecto, el Supervisor solicitará la modificación de dicho personal, lo cual deberá ser acatado por el contratista en un plazo máximo de 3 días hábiles, este personal deberá contar con iguales o superiores condiciones de formación y experiencia y debe ser aprobado por el supervisor. • Suministrar el personal técnico y especializado que se requiera para el cumplimiento del objeto contractual, sin importar el número de profesionales requeridos, y sin que se genere costo adicional para la Entidad, conforme a los lineamientos y directrices impartidos por la supervisión del contrato. • Presentar a la Entidad las opciones de configuración disponibles para las soluciones tecnológicas adquiridas, y recomendar a la supervisión del contrato aquella(s) que mejor se adecue(n) a las necesidades de la plataforma tecnológica y permitan un mejor uso y desempeño de las soluciones adquiridas.
5.2	Nivel de soporte Requerido.

Anexo 1 - FICHA TÉCNICA

	1. El nivel de soporte en este ítem debe ser tenido en cuenta durante los periodos de garantía estándar y extendida solicitados en el proceso. 2. Nivel de atención requerido: 24x7x365. 3. Registro de incidentes a través de los siguientes canales de servicio: • Telefónico. • Chat en Línea. • Correo electrónico • Plataforma propia de la solución ofrecida. 4. Mantenimiento preventivo: Actualización de versiones y release de software de mantenimiento y versiones menores para los equipos y software cubiertos; debe incluir acompañamiento en la actualización en caso de que dicho upgrade sea requerido para resolver un incidente. 5. Asesoría en uso de las herramientas de diagnóstico y de resolución de problemas. 6. Respuesta rápida en caso de emergencia por medio de acceso remoto por Internet. 7. Soporte remoto para diagnóstico y detección de fallas de hardware y software. 8. Soporte de requerimientos de consulta sobre productos, operación o mantenimiento. Alcance según Nivel de Servicio: a) Asistencia inmediata a través del punto de contacto de soporte, disponible las veinticuatro (24) horas del día, los siete (7) a la semana, todo el año, en un lapso no superior a 30 minutos, categorizando el tipo de impacto de la incidencia o el problema (Muy crítico [Prioridad 1], fallo total o parcial que impida el funcionamiento de la solución; Crítico [Prioridad 2]: Fallo que impacte la operatividad pero no de forma catastrófica, Media [Prioridad 3]: fallo de algún componente de hardware o Software que no genere impacto en la operación). b) El oferente dispondrá de personal técnico especializado en horario 24x7 (las 24 horas de día, 7 días a la semana) para atender las solicitudes del cliente (incidentes o fallas) y realizar el diagnóstico, y de ser necesario por la característica del problema, el escalamiento correspondiente al fabricante. c) Asistencia en sitio o remota dentro de las 6 horas siguientes al reporte del problema para incidentes de prioridad 1, de 8 horas hábiles para incidentes de prioridad 2 y de 10 Horas hábiles para incidentes de prioridad 3. d) Suministro de partes dentro de las 6 horas siguientes una vez realizado el diagnóstico y confirmada la falla de hardware por el personal técnico especialista del fabricante.
5.3	Transferencia de conocimiento. La transferencia debe realizarse sobre los 2 componentes de hardware: 1. Solución HCI 2. Solución de backup Se requiere una transferencia de conocimiento no certificada por parte del oferente adjudicatario del proceso con las siguientes características:

Anexo 1 - FICHA TÉCNICA

	1. La instalación, configuración y puesta en marcha de la solución de Hiperconvergencia, debe incluir la transferencia de conocimiento en su operación durante mínimo 10 horas de y hasta para 5 funcionarios designados por la supervisión, necesaria para la administración de la totalidad de herramientas que integran la solución HCI. Esta deberá ser construida y presentada por el oferente, conteniendo los temas necesarios para la apropiación técnica del proyecto y deberá ser aprobada por el supervisor del contrato. Para este ítem se incluye el software del Hipervisor el cual también deberá estar incluido en esta transferencia. 2. La instalación, configuración y puesta en marcha de la solución de Backup, debe incluir la transferencia de conocimiento en su operación durante mínimo 10 horas de y hasta para 5 funcionarios designados por la supervisión, necesaria para la administración de la totalidad de herramientas que integran la solución de Backup. Esta deberá ser construida y presentada por el oferente, conteniendo los temas necesarios para la apropiación técnica del proyecto y deberá ser aprobada por el supervisor del contrato. Para este ítem se incluye el software de gestión de copias de respaldo el cual también deberá estar incluido en esta transferencia.
--	--

Proyectó: Equipo Técnico GIT TIC's Mindeporte.

Actualizado: junio de 2026.
Datacenter 0106202

Enterado, aceptamos y cumplimos



Jesús Alberto Franco Acosta

C.E. 582410

Representante Legal

HEIMCORE SAS