

**“ADQUISICIÓN DEL SISTEMA HIPERCONVERGENTE PARA EL  
FORTALECIMIENTO DEL PROCESAMIENTO DE APLICACIONES Y  
GESTIÓN DE RESPALDOS DEL CENTRO DE DATOS DEL MINISTERIO  
DE SALUD PÚBLICA”**

**1. DESCRIPCIÓN DEL BIEN/SERVICIO**

**1.1. Lista de Bienes y Servicios:**

Se requiere adquirir los siguientes bienes y servicios, según las cantidades indicadas en las siguientes tablas:

**Bienes**

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD REQUERIDA
1	Hardware	Sistema Hiperconvergente y sus respectivos Subsistemas  Incluye: -Mínimo siete (7) nodos hiperconvergentes. -Instalación, configuración y puesta en marcha; -Materiales e implementación del cableado y rieles de montaje; - Garantía técnica de fábrica; - Soporte técnico; - Licenciamiento de Sistema Operativo; - Software de Orquestación de Respaldos.	1
2	Hardware	Switches LAN para Integración de Sistema Hipercovergente y red de administración  Incluye: -Instalación, configuración y puesta en marcha de los equipos; -Materiales e implementación del cableado y rieles de montaje; - Garantía técnica de fábrica; - Soporte técnico.	4
3	Hardware	Solución de Almacenamiento para Respaldos  Incluye: -Instalación, configuración y puesta en marcha del equipo; -Materiales e implementación del cableado y rieles de montaje; - Garantía técnica de fábrica; - Soporte técnico.	1

## Servicios Conexos

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD REQUERIDA
4	Servicio	Movimiento de máquinas virtuales	300

### 1.2. Detalle de Especificaciones Técnicas

En las especificaciones técnicas del sistema hiperconvergente se hará referencia a los siguientes componentes:

Componente	Descripción
Sistema Hiperconvergente	<ul style="list-style-type: none"> <li>• Sistema Hiperconvergente</li> <li>• Nodos hiperconvergentes (hardware de nodos del sistema hiperconvergente)</li> <li>• Virtualización de Cómputo (software del sistema hiperconvergente)</li> <li>• Virtualización Almacenamiento (software del sistema hiperconvergente)</li> <li>• Gestión Virtualización (software del sistema hiperconvergente)</li> <li>• Gestión de Seguridad (software de seguridad del sistema hiperconvergente)</li> <li>• Gestión del Ciclo de Vida (software del sistema hiperconvergente)</li> <li>• Licenciamiento de Sistema Operativo</li> <li>• Software de Orquestación de Respaldos</li> </ul>
Equipos de conectividad	<ul style="list-style-type: none"> <li>• Switches LAN para Integración de Sistema Hiperconvergente</li> <li>• Switches LAN para Red de Administración</li> </ul>
Solución de Almacenamiento para Respaldos	Solución de Almacenamiento para Respaldos

#### 1.2.1. Sistema Hiperconvergente

SISTEMA HIPERCONVERGENTE	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Actualizaciones	Las actualizaciones de software, firmware, parches/fixes deberán ser entregadas por el fabricante del sistema hiperconvergente en forma integrada y automatizada, considerando todos los componentes, excepto el Sistema Operativo. No podrán ser aplicadas actualizaciones y/o parches por separado que no hayan sido pre validados por el fabricante del sistema hiperconvergente y liberadas por el fabricante del software de hiperconvergencia.
Soporte	El sistema deberá contar con una aplicación/herramienta de soporte que reporte el estado/fallas de los equipos o componentes que lo conforman, directamente al fabricante del sistema hiperconvergente en forma automática y unificada tanto para el hardware como para el software.
Tipo	<p>El sistema hiperconvergente ofertado deberá ser catalogado como "Sistema Integrado", donde todos sus componentes están constituidos como un solo producto e integrados en fábrica, no como componentes separados, información que deberá estar publicada en la página web oficial del fabricante, así como en datasheet del producto. No se aceptarán nodos compatibles, nodos certificados, ni los denominados "Ready Nodes". Adjuntar certificado del fabricante que avale lo solicitado.</p> <p>El proveedor podrá integrar únicamente productos de máximo dos fabricantes de hardware para este proyecto, esto con la finalidad de simplificar la gestión y el soporte técnico.</p>
Escalabilidad	El sistema hiperconvergente deberá tener la capacidad de expansión tanto de forma vertical para capacidad de almacenamiento como horizontal para capacidades de cómputo, memoria y almacenamiento con incremento en el número de nodos.

SISTEMA HIPERCONVERGENTE	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Licenciamiento	El licenciamiento de todos los componentes de software que conforman el sistema hiperconvergente excepto del Sistema Operativo, deberán venir integrados desde fábrica con los nodos hiperconvergentes. Todo licenciamiento deberá estar registrado a nombre del Ministerio de Salud Pública. Deberá incluir los servicios de soporte y suscripción del fabricante del Sistema Hiperconvergente, por el tiempo de vigencia de la garantía técnica. Los servicios de soporte y suscripción del licenciamiento requerido, deberán permitir al Ministerio de Salud Pública la descarga y actualización de nuevas versiones del software estable liberado por el fabricante para todos los productos detallados en este documento.

### 1.2.1.1. Nodos hiperconvergentes

NODOS HIPERCONVERGENTES	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Descripción	<p>Los nodos del sistema hiperconvergente se deberán configurar como mínimo con el siguiente pool de recursos usables en el clúster HCI, por el Ministerio de Salud Pública:</p> <ul style="list-style-type: none"> <li>Total, de recursos de procesamiento mínimo usable requerido: 806 GHz (velocidad de procesador frecuencia base * # cores físicos totales por nodo * # nodos ofertados)</li> <li>La frecuencia base de cada procesador no deberá ser menor a 3.6GHz</li> <li>La cantidad total mínima requerida de cores físicos por el clúster es de mínimo 224 cores sin aplicar hilos de procesamiento.</li> <li>La cantidad mínima requerida de cores físicos por procesador deberá ser de mínimo 16.</li> <li>Memoria usable mínimo: 14TB en el cluster, 2TB por nodo (con módulos de mínimo 64GB RDIMM).</li> <li>Capacidad en disco: Se deberá entregar una capacidad usable de almacenamiento All-Flash de mínimo 200 TB útiles, sin considerar parámetros de compresión ni de-duplicación. El proveedor deberá considerar mandatoriamente la configuración de protección de fallas RAID-6, requerida por el Ministerio de Salud Pública para la entrega de la capacidad mínima usable solicitada en este apartado.</li> </ul> <p><b>Nota Importante:</b> Se podrá considerar el aumento/incremento del número de nodos, procesadores por nodo, características técnicas de procesadores y/o demás componentes que se requieran, para entregar el pool de recursos usable mínimo requerido en este apartado, dentro de su sistema hiperconvergente ofertado.</p>
Marca	Especificar
Modelo	Especificar
Cantidad	El contratista deberá incluir como mínimo siete (7) nodos hiperconvergentes.
Formato	Rack 2U cada nodo
Tolerancia a fallos	Deberá soportar la caída de máximo 2 nodos (FTT=2)
Escalabilidad	El sistema hiperconvergente deberá tener una escalabilidad de mínimo hasta sesenta y cuatro (64) nodos Deberá permitir incrementar memoria RAM, discos de Caché, discos de datos y tarjetas de I/O de acuerdo con la disponibilidad del hardware ofertado.
Procesador	<p>Cada nodo hiperconvergente deberá contar como mínimo con las siguientes características de procesadores:</p> <ul style="list-style-type: none"> <li>Los procesadores a ofertar deben ser los últimos liberados por el fabricante, teniendo en cuenta las especificaciones mínimas solicitadas.</li> <li>Mínimo dos (2) procesadores, de acuerdo con la arquitectura y/o cantidad de nodos requerida, y al cumplimiento del pool de recursos solicitados por el Ministerio de Salud Pública.</li> <li>Segmento: Para servidores.</li> <li>Mínimo 16 núcleos (cores) por cada procesador.</li> <li>Mínimo 3.6GHz de frecuencia base.</li> <li>Mínimo 45MB de Cache.</li> <li>Conjunto de instrucciones de 64-bits.</li> </ul>

NODOS HIPERCONVERGENTES	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
	<ul style="list-style-type: none"> <li>Hilos por núcleo (core): mínimo 2 hilos de procesamiento por núcleo (core).</li> <li>Procesadores escalables de mínimo cuarta generación o de generación superior.</li> <li>Familia 6400 o superior.</li> </ul>
Memoria	Cada nodo hiperconvergente deberá incluir como mínimo 2TB de memoria RAM usable por el Ministerio de Salud Pública, para el despliegue y/o asignación a sus máquinas virtuales; con módulos de mínimo 64GB de tipo DDR5 o de tecnología superior, de mínimo 4800 MT/s de velocidad. Cada nodo hiperconvergente deberá disponer de mínimo 32 slots para memoria RAM asignable. En todos los casos el contratista deberá considerar la cantidad de memoria RAM necesaria para cumplir con el pool de recursos usables totales requeridos por el Ministerio de Salud Pública.
Discos	Cada nodo hiperconvergente deberá contar como mínimo con la siguiente capacidad de almacenamiento all-flash instalada: <ul style="list-style-type: none"> <li>Cache: Mínimo dos (2) discos NVMe Mixed Use de mínimo 1.6TB, o de tecnología superior cada nodo.</li> <li>Datos: Mínimo ocho (8) discos cada uno de mínimo 7.68TB SSD SAS o de tecnología superior.</li> <li>El almacenamiento requerido deberá configurarse en mínimo dos grupos de discos y deberá permitir crecer en la cantidad de grupos de discos. Deberá contar con mínimo 24 bahías para dispositivos de almacenamiento SAS/SATA/NVMe (HDD/SSD)</li> <li>En todos los casos el contratista deberá considerar las recomendaciones dispuestas por el fabricante de los equipos para la configuración de la capacidad de almacenamiento requerida en este apartado.</li> </ul>
Interfaces de red LAN	<ul style="list-style-type: none"> <li>Como mínimo dos tarjetas de dos puertos 25GbE SFP28 cada una, con la finalidad de garantizar rendimiento y redundancia a nivel de componente físico. Cada tarjeta deberá incluir todos los Transceivers y/o cables Twinax requeridos para la interconexión.</li> <li>Mínimo un (1) puerto a 1Gb Ethernet o velocidad superior para la Gestión/Administración nivel empresarial.</li> </ul>
Interfaces de red SAN	<ul style="list-style-type: none"> <li>Como mínimo una tarjeta HBA de dos puertos FibreChannel a 32Gbps que también soporte 16Gbps, para conexión a switches SAN Fibre Channel existentes en el Ministerio de Salud Pública.</li> </ul>
Ventilación	Redundante
Alimentación de poder	Redundante

### 1.2.1.2. Virtualización de computo

VIRTUALIZACIÓN DE COMPUTO	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Marca	Especificar
Modelo	Especificar
Cantidad	Especificar
Marco de análisis	La solución de virtualización deberá constar en el cuadrante de líderes de Gartner como mínimo durante el año 2020 o año superior en la categoría de Software para Infraestructura Hiperconvergente.
Licenciamiento	El sistema hiperconvergente deberá incluir el licenciamiento y suscripción para la plataforma de virtualización, para toda la cantidad de procesadores por nodo ofertados. El proveedor deberá detallar las especificaciones de licenciamiento/suscripción propuesta. Todo licenciamiento deberá ser estar registrado a nombre del Ministerio de Salud Pública.
Despliegue	Se deberá instalar la última versión del software de plataforma de virtualización liberada por el fabricante del software y soportada por el fabricante del sistema hiperconvergente. El proveedor deberá sustentar lo requerido en este apartado, con un certificado emitido por el fabricante del

VIRTUALIZACIÓN DE COMPUTO	
	sistema hiperconvergente y con un certificado del fabricante del software de la plataforma de virtualización en donde se indique cual es la última versión.
Compatibilidad	El sistema hiperconvergente ofertado deberá ser 100% compatible con la actual plataforma de virtualización del Ministerio de Salud Pública. (VMware vSphere). El Sistema Hiperconvergente deberá incluir y venir precargado de fábrica con el software Hipervisor, esto con la finalidad de disminuir los tiempos de puesta en marcha. El hipervisor ofertado deberá ser 100% compatible con la infraestructura virtual y/o hipervisores que actualmente dispone el Ministerio de Salud Pública en su infraestructura física y el tipo de licenciamiento deberá ser entregado sobre la última versión/edición disponible, estable y compatible del hipervisor, esto con la finalidad de contar con todas las funcionalidades liberadas por el fabricante. El hipervisor ofertado deberá permitir el monitoreo/administración con herramientas propias del fabricante mediante una consola virtual independiente y de propósito específico, sin límite de Máquinas Virtuales. El proveedor deberá incluir todo el licenciamiento requerido para la instalación y uso de la herramienta de administración de la solución de virtualización.
Soporte	El fabricante del sistema hiperconvergente requerido en este documento deberá proveer del soporte integrado de la capa de virtualización de cómputo. El Ministerio de Salud Pública se reserva el derecho de solicitar la apertura de casos de soporte de la capa de virtualización y demás componentes de software/firmware solicitados en este documento a través del proveedor de la solución o directamente a través del fabricante del sistema hiperconvergente (se exceptúa el soporte en el licenciamiento Red Hat Linux requerido).
Alta disponibilidad	El hipervisor deberá incluir funcionalidades de alta disponibilidad.
Tolerancia a fallos	El hipervisor deberá permitir la disponibilidad continua de cualquier aplicación en caso de falla de hardware, sin pérdida de datos ni tiempo de inactividad.
Información de estadísticas	La solución deberá permitir entregar estadísticas completas sobre las máquinas virtuales, como consumos de CPU, RAM y Almacenamiento, así como los IOPs de lectura/escritura y latencias.
Características de la plataforma de virtualización de cómputo	La plataforma de virtualización de cómputo deberá contar con el mayor nivel de funcionalidades desarrolladas por el fabricante del software de hiperconvergencia. En términos generales deberá cumplir como mínimo con las siguientes especificaciones técnicas: <ul style="list-style-type: none"> <li>• Permitir la migración en vivo/caliente de las máquinas virtuales de un nodo a otro.</li> <li>• Permitir la migración en vivo/caliente de los datastore de un almacenamiento o LUN a otra.</li> <li>• Permitir la configuración de alta disponibilidad</li> <li>• Reinicio automático de máquinas virtuales después de una falla de la máquina física.</li> <li>• Permitir el incremento de recursos de CPU y RAM de las máquinas virtuales, en caliente</li> <li>• Integración con agentes de respaldos para recuperación de máquinas virtuales.</li> <li>• Soportar la capacidad de replicación a través de red LAN y WAN.</li> <li>• Capacidad de recuperarse ante una falla de sistema operativo o aplicación.</li> <li>• Permitir capturar la configuración de un nodo virtual para poder cargarlo a otro.</li> <li>• Permitir el movimiento de máquinas virtuales entre nodos de hiperconvergencia en caliente.</li> <li>• Permitir el movimiento de máquinas virtuales entre zonas de almacenamiento en caliente</li> <li>• Permitir migrar automáticamente las máquinas virtuales durante el mantenimiento sin interrumpir el servicio.</li> <li>• Permitir implementar capacidad nueva en el clúster sin interrumpir el servicio.</li> <li>• Permitir el equilibrio de carga automático entre los hosts que conforman el clúster.</li> </ul>

### 1.2.1.3. Virtualización de almacenamiento

VIRTUALIZACIÓN DE ALMACENAMIENTO	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Marca	Especificar
Software integrado	El sistema hiperconvergente solicitado en este documento deberá incluir un software integrado y precargado de virtualización de almacenamiento (hiperconvergencia). El proveedor deberá detallar las especificaciones del software integrado.
Licenciamiento	Todo licenciamiento deberá ser perpetuo y registrado a nombre del Ministerio de Salud Pública. Deberá incluir los servicios de soporte y suscripción de fabricante por el tiempo de vigencia de la garantía técnica. Los servicios de soporte y suscripción del licenciamiento requerido, deberán permitir al Ministerio de Salud Pública la descarga y actualización de nuevas versiones del software estable liberado por el fabricante para todos los productos detallados en este documento.

Soporte	El fabricante del sistema hiperconvergente requerido en este documento deberá proveer del soporte integrado de la capa de virtualización de almacenamiento. El Ministerio de Salud Pública se reserva el derecho de solicitar la apertura de casos de soporte de la capa de virtualización de almacenamiento y demás componentes de software/firmwares solicitados en este documento a través del proveedor de la solución o directamente a través del fabricante del sistema hiperconvergente (se exceptúa el soporte en el licenciamiento Red Hat Linux requerido).
Características de la plataforma de virtualización de almacenamiento	<p>La capa de virtualización de almacenamiento deberá correr en el mismo kernel del hipervisor a fin de optimizar el uso de los recursos y asegurar rendimiento, esto significa que la funcionalidad de virtualización de almacenamiento deberá ser parte del kernel y por tanto embebida en el mismo. No se deberá ejecutar como un controlador por fuera del kernel del hipervisor en máquinas virtuales.</p> <p>La administración de la virtualización de almacenamiento deberá ser integrada a la administración de virtualización de cómputo y no ser una consola independiente.</p> <p>El sistema de almacenamiento deberá manejar, como políticas, las siguientes características técnicas mínimas:</p> <ul style="list-style-type: none"> <li>• Desempeño</li> <li>• Nivel de protección</li> <li>• Calidad de Servicio</li> </ul> <p>Estas características deberán tener la granularidad a nivel de máquina virtuales.</p>
Funcionalidades de la plataforma de virtualización Almacenamiento	<p>Las funcionalidades del almacenamiento del sistema hiperconvergente ofertado deberá soportar como mínimo las siguientes funcionalidades:</p> <ul style="list-style-type: none"> <li>• Hardware All-Flash</li> <li>• Replicación</li> <li>• Protección contra fallas locales</li> <li>• Proveer recursos de bloques a sistemas fuera del sistema hiperconvergente, a través de protocolos estándares como iSCSI.</li> <li>• Calidad de servicio</li> <li>• De-duplicación</li> <li>• Compresión</li> <li>• Protección RAID-5/6</li> </ul> <p>Las funcionalidades del almacenamiento deberán incluir y configurarse con soporte para la de-duplicación y compresión de datos.</p>
Despliegue	Las funcionalidades del almacenamiento deberán venir precargadas de fábrica y podrán ser activadas durante la implementación, de así requerirlo el Ministerio de Salud Pública.

#### 1.2.1.4. Gestión de Virtualización

GESTION DE VIRTUALIZACIÓN	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Funcionalidades	Las funciones de administración de cómputo y almacenamiento virtualizado deben ser integradas en una sola consola.
Licenciamiento	Todo licenciamiento deberá ser estar registrado a nombre del Ministerio de Salud Pública. Deberá incluir los servicios de soporte y suscripción de fabricante por el tiempo de vigencia de la garantía técnica. Los servicios de soporte y suscripción del licenciamiento requerido, deberán permitir al Ministerio de Salud Pública la descarga y actualización de nuevas versiones del software estable liberado por el fabricante para todos los productos detallados en este documento.
Consola	<p>Deberá proveerse una consola integrada tipo GUI para realizar funciones de gestión.</p> <p>El sistema hiperconvergente deberá permitir ser gestionado desde una consola con mínimo las siguientes funcionalidades:</p> <ul style="list-style-type: none"> <li>• Gestionar todos los componentes de la solución hiperconvergente.</li> <li>• Gestionar el clúster de recursos centralizadamente.</li> <li>• Soporte para monitoreo de los hipervisores centralizadamente.</li> <li>• Aprovisionar recursos.</li> <li>• Asignar roles de usuario basado en perfiles por lo que la solución soportará la integración con Directorio Activo o con sistemas LDAP para la autenticación en el uso de la herramienta.</li> <li>• Deberá tener interfaz gráfica de administración basada en un entorno WEB</li> </ul>

		<p>La interfaz gráfica deberá entregar mínimo estadísticas completas sobre las máquinas virtuales como consumos de vCPUs, Memoria RAM y discos, así como: IOPS de lectura, IOPS de escritura y métricas de red.</p> <p>La solución deberá permitir analizar en forma gráfica el impacto que tiene un evento con el comportamiento de la plataforma global y/o con el comportamiento de una máquina virtual a nivel de CPU, memoria, disco y red.</p> <p>La interfaz gráfica de administración deberá tener la capacidad de configurar roles de usuario, como mínimo rol operador y rol administrador. La solución soportará la integración con Directorio Activo o con sistemas de LDAP para la autenticación en el uso de la herramienta.</p>
Análisis de Capacidad	de	Proporcionar análisis de capacidad que puede identificar los recursos que tenemos sobre aprovisionados de manera que sea posible ajustarlos (Right-Sizing) y facilitar mantener el entorno en estado eficiente.
Reporte de Capacidades	de	Generar reportes de capacidades para proporcionar una visibilidad profunda de las tendencias de consumo de recursos capacidad (forecast) de modo que sea posible anticiparse a los requerimientos futuros de recursos.
Vistas informes prediseñados	e	Proporcionar vistas e informes prediseñados y que sean configurables sus cuadros de mando, además la información se deberá de desplegar en tiempo real para proporcionar información sobre el comportamiento de infraestructura, diagnosticar los problemas que surjan, y manejo de oportunidades para mejorar la eficiencia.
Análisis de capacidad	de	Permitir realizar análisis de capacidad y deberá proporcionar diferentes tipos de escenarios hipotéticos (tipo de "What If") para simplificar la gestión de capacidades futuras, y eliminar la necesidad de hojas de cálculo, y manejo de scripts.
Análisis de rendimiento	de	Generar análisis de rendimiento de autoaprendizaje y umbrales dinámicos que pueden adaptarse al medio para simplificar la gestión de las operaciones, así como construir alertas basadas en más de un síntoma (súper métricas), esto con el objetivo de disminuir las falsas alertas e incrementar la eficiencia operacional.
Control de recursos	de	Permitir controlar tanto los recursos físicos de hardware como sistemas operativos, de modo que sea posible gestionar tanto la infraestructura virtual y física con una única solución.
Extensión de capacidades	de	Se deberá permitir extender estas capacidades con herramientas de terceros, como Sistemas Operativos, Base de Datos (por ejemplo: MySQL, MS SQL Server, Oracle DB), Aplicaciones (por ejemplo: Apache Tomcat, MS IIS), Red (switches, firewall, enrutadores, balanceadores) y almacenamiento tradicional.
Aseguramiento		Proveer plantillas para visibilizar el aseguramiento del entorno (hardening), así como cambios, configuraciones y cumplimiento normativo, y de esta forma disminuir el riesgo ante potenciales fisuras de seguridad.
Operaciones Inteligentes		Permitir la creación de grupos de operaciones inteligentes y poder manejar diferentes categorías de usuarios, así como diferentes tipos de privilegios, y poder crear Grupos de forma dinámica ó estática y/o Mixta, la cual nos ayuda a tener una mejor administración de los equipos. También deberá de contar con diferentes formas de acceder a la herramienta, como puede ser: AD, LDAP, usuarios locales, etc.
Gestión de registros	de	Deberá proveer un sistema de gestión de registros (logs) para el entorno hiperconvergente, pero que pueda recibir logs de otros entornos. Deberá permitir la gestión logs de forma unificada, de forma intuitiva, con tableros de mando (dashboards) y capacidades de análisis sofisticados.
Alarmas		Deberá proveer la funcionalidad de alarmas preventivas y automáticas en caso de falla de componentes del sistema a través de correo electrónico. Deberá permitir determinar en tiempo real el consumo de los recursos de CPU, Memoria RAM y almacenamiento por nodo, por máquina virtual, para el clúster y en forma global. La solución deberá estar en la capacidad de emitir alertas en caso de problemas detectados a nivel de hardware y software. La solución deberá permitir configurar umbrales para la emisión de alertas, así como su criticidad (como mínimo 3 categorías: crítica, warning y normal).
Gestión		El sistema hiperconvergente deberá contar con un software de gestión que mínimo cumpla con las siguientes funcionalidades: <ul style="list-style-type: none"> <li>• Descubrir y mantener automáticamente el inventario de toda la infraestructura del sistema.</li> <li>• Chequeo de las versiones de software instaladas en el sistema versus las versiones de software certificadas por el fabricante.</li> <li>• Logs del sistema hiperconvergente.</li> <li>• Monitoreo del estado de salud de la infraestructura.</li> </ul> <p>La solución propuesta deberá incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada en los nodos que componen la solución, manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información.</p>
Mecanismo de actualización	de	La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, cómputo e Hipervisor) directamente desde la consola

	WEB y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni ocurrencia de indisponibilidad del servicio.
Integración	La solución deberá soportar integración mediante el uso de REST API, SNMP, Web Services u otros similares que habilite la integración a otras soluciones de administración para facilitar la integración con ambientes de monitoreo actuales.
Análisis de ancho de banda	La solución deberá permitir el análisis de ancho de banda utilizado por una máquina virtual, un host físico, o un clúster.
Capacidad	La solución deberá poder brindar información en formatos CSV de mínimo: <ul style="list-style-type: none"> <li>• Capacidad por clúster.</li> <li>• Capacidad por nodo.</li> <li>• Rendimiento por clúster.</li> <li>• Rendimiento por nodo.</li> <li>• Rendimiento por máquina virtual o por grupo de máquinas virtuales.</li> <li>• Alertas presentadas.</li> </ul>
Integración nativa con el sistema de gestión	Deberá tener integración nativa con el sistema de gestión, de modo que sea posible relacionar las métricas del entorno con los eventos (logs) y poder simplificar las operaciones de resolución de problemas o análisis de causa-raíz.

### 1.2.1.5. Gestión de Seguridad

GESTION DE SEGURIDAD	
ATRIBUTOS	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Modelo	No será permitido un modelo de virtual appliance para el control e inspección del tráfico de una máquina virtual a otra máquina virtual (inter VM's)
Firewall Distribuido	La solución de Firewall distribuido deberá ser gestionada a través de una única consola central y deberá ofrecer la protección e inspección del tráfico que ocurre en todas las máquinas virtuales a nivel de vNIC (tarjeta de red virtual). El Firewall distribuido deberá operar en modalidad transparente y en el kernel del hipervisor, sin la necesidad de cambiar ningún atributo de las máquinas virtuales como dirección IP o default Gateway para su operación. Cada vez que se integra un nuevo nodo (hipervisor) al ambiente, el componente de firewall distribuido podrá ser habilitado de manera automática. Deberá proveer la capacidad de firewall perimetral como Virtual Appliance para el tráfico de entrada y salida del ambiente de las máquinas virtuales a la infraestructura física, también conocido como tráfico Norte-Sur.
Soporte	La solución deberá soportar la plataforma de virtualización VMware vSphere deberá implementar la capacidad de firewall distribuido a nivel del kernel del hipervisor brindando así protección a todo el entorno virtualizado. El componente de Firewall distribuido deberá admitir la seguridad de las máquinas virtuales conectadas a los grupos de puertos virtuales distribuidos. El firewall distribuido deberá soportar la definición de reglas desde capa 2 (MAC Address), capa 3 (IP Origen/Destino) y capa 4 (TCP, UDP, ICMP, protocolos IP). Deberá Soportar la definición de mínimo 120000 reglas por hipervisor del host.
Capacidad de inspección	Cada hipervisor deberá proveer una capacidad de inspección en firewall de mínimo 20Gbps, y deberá soportar escalabilidad horizontal (scale-out).
Micro segmentación	Las capacidades de micro segmentación deberán permitir aislar bajo un modelo de seguridad "zero trust" o cero confianza y únicamente permitir el tráfico permitido entre máquinas virtuales, al nivel de bloquear incluso la comunicación de máquinas que se encuentren en el mismo segmento lógico o VLAN. La solución de micro segmentación deberá ser integrable a través de API's REST para la creación, modificación o eliminación de políticas de seguridad utilizando plataformas de gestión de nube, software de terceros o herramientas de automatización.
Certificación	El firewall distribuido deberá ser certificado por ICSA Labs.
Inspección	El firewall distribuido deberá realizar inspección del estado de conexiones, mejor conocido como "stateful inspection", descartando en automático comunicaciones que no hayan sido identificadas y autorizadas previamente Deberá permitir que la inspección del firewall sea aplicada tanto a nivel del perímetro del Data Center virtual, así como al nivel de interfaz de red (vNIC) de cada máquina virtual. La tabla de reglas del firewall distribuido deberá permitir la automatización con objetos propios de la infraestructura virtual.



Detección de paquetes	Deberá descartar en automático paquetes mal formados o que intenten suplantar una conexión existente. Deberá soportar fragmentación de paquetes.
Integración	El firewall distribuido tendrá la capacidad de integrarse con grupos de Microsoft Active Directory para ofrecer el servicio de Firewall basado en identidad.
Gestión de registros	El firewall distribuido deberá tener la capacidad de generar registros de eventos (logs) y deberá contar con una herramienta propia para el monitoreo de registros de seguridad (logs) generadas por las instancias de firewall distribuido.
Gestión de reglas	Deberá contar con una única interface para la gestión de las reglas del firewall distribuido, de igual manera, la administración y definición de reglas deberá ser realizada utilizando objetos nativos del hipervisor para origen y/o destino tales como: <ul style="list-style-type: none"> <li>• Dirección IP: Origen y Destino</li> <li>• Puertos: Origen y Destino</li> <li>• Protocolo y Tipo: TCP/UDP/ICMP, etc.</li> <li>• DataCenter</li> <li>• Cluster</li> <li>• Red Virtual</li> <li>• Aplicación Virtual</li> <li>• Asociación de recursos (Resource Pool)</li> <li>• Máquina Virtual</li> <li>• Interfaz de red a nivel máquina virtual</li> <li>• Grupo de seguridad.</li> <li>• Sistema Operativo</li> <li>• Etiquetas o tags de seguridad</li> </ul>
Aplicación de reglas	Deberá permitir aplicar las reglas de firewall distribuido de manera general a particular, es decir, se podrán definir reglas que apliquen a toda la infraestructura virtualizada, y reglas puntuales que sean aplicadas a máquinas virtuales, interfaces virtuales (vNICs) de manera específica. Deberá permitir reglas de protección que sean aplicadas a una red específica, puerto de aplicación, tipo de protocolo (TCP/UDP) o tipo de aplicación.
Agrupamiento	Deberá soportar el agrupamiento estático y dinámico de objetos para la creación de grupos de seguridad de manera eficiente.
Grupos de Seguridad	Deberá permitir el anidamiento de grupos de seguridad. Deberá tener la capacidad de modelar grupos de seguridad.
Políticas de Seguridad	El firewall distribuido deberá aplicar las políticas de seguridad sobre las máquinas virtuales, sin importar si las máquinas son migradas o movidas de un host a otro. De igual forma, en caso de borrar una máquina virtual, la(s) regla(s) asociada(s) a dicha máquina virtual serán eliminadas, reduciendo así riesgos de seguridad por políticas mal aplicadas. Deberá tener la capacidad de proponer políticas de seguridad que podrán ser exportadas como políticas de micro segmentación en la infraestructura de virtualización.
Interfaz	Deberá contar con herramientas de línea de comando que faciliten el análisis y troubleshooting. Deberá proveer una interfaz de búsqueda intuitiva y de auto-completamiento que permita definir criterios de búsqueda básicos y/o complejos.
Monitoreo	Deberá contar con monitoreo granular del tráfico para una respuesta rápida y resolución de problemas, así como proveer contadores de tráfico para las sesiones, paquetes y bytes para favorecer la visibilidad dentro de la red virtual, así como la creación de reglas de firewall. Deberá proveer capacidades analíticas basadas en el contexto de la infraestructura de virtualización que incluya los componentes de cómputo, redes, seguridad, conectividad física, virtual y de nube, mapeado y/o asociar las cargas de trabajo a las redes, sean por VLAN. La solución deberá coleccionar información de configuración, tablas de ruteo, entre otros de dispositivos físicos de comunicación de fabricantes líderes a partir de protocolos como SSH o SNMP. Deberá poder crear alertas a partir de violaciones a parámetros definidos. Deberá tener la capacidad de retener el histórico de flujos con un aproximado de un mes.
Bloqueo discrecional	Deberá contar con un mecanismo que permita identificar la impersonación de MAC Address o IP en las máquinas virtuales (IP/Mac Spoofing) para realizar bloqueo discrecional de este tipo de comunicaciones.
Compatibilidad	Deberá ser compatible con el entorno de hiperconvergencia que se solicita en el presente proceso, con el fin de tener una visibilidad extendida (infraestructura y red).
Licenciamiento	Se deberá incluir el licenciamiento/suscripciones que deberá ser registrado a nombre del Ministerio de Salud Pública. Deberá incluir los servicios de soporte y suscripción de fabricante por el tiempo de vigencia o la garantía técnica. Los servicios de soporte y suscripción del licenciamiento requerido deberán permitir al Ministerio de Salud Pública la descarga y actualización de nuevas versiones del software estable liberado por el fabricante. Al ser un entorno dinámico, el licenciamiento/suscripciones deberá estar basado en procesador (sockets o cores). Se deberá considerar la cantidad de procesadores (sockets o cores) instalados en el sistema hiperconvergente para el dimensionamiento del licenciamiento de la solución de seguridad.

### 1.2.1.6. Gestión del Ciclo de vida

GESTIÓN DEL CICLO DE VIDA	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Licenciamiento	El proveedor deberá incluir el licenciamiento/suscripciones que deberá ser registrado a nombre del Ministerio de Salud Pública. Deberá incluir los servicios de soporte y suscripción de fabricante por el tiempo de vigencia de la garantía técnica. Los servicios de soporte y suscripción del licenciamiento requerido, deberán permitir al Ministerio de Salud Pública la descarga y actualización de nuevas versiones del software estable liberado por el fabricante.
Interfaz	La solución deberá incluir una interfaz que gestione la infraestructura y que pueda aprovisionar nuevos recursos, construyendo la base para una nube privada.
Automatización	La solución podrá automatizar todo el ciclo de vida del sistema (desde la configuración y el aprovisionamiento hasta las actualizaciones y parches), y así simplificar la administración y las operaciones diarias, desde un único punto de administración. Es decir, deberá realizar tareas tales como: Gestionar certificados y contraseñas, adicionar capacidad al sistema, configurar y aprovisionar los sistemas y los dominios de carga de trabajo, gestionar dominios de carga de trabajo aprovisionados, monitorear alertas y la salud del sistema, detectar problemas física y virtual y realizar la gestión del ciclo de vida en los componentes de software.
Gestión	La plataforma deberá incluir un gestor que provea las funciones de automatizar todo el ciclo de vida; despliegue, configuración, aplicación de parches y actualizaciones del sistema y que simplifique las operaciones de software, y que además permita extender de forma unificada las actividades anteriores hacia los componentes de hardware.
Entendimiento de Topología	El gestor deberá ser capaz de entender la topología física y lógica del centro de datos definido por software (SDDC), así como la relación existente entre los componentes subyacentes y supervisar eficientemente la infraestructura para detectar posibles riesgos, degradaciones y fallos.
Monitoreo	La solución deberá proporcionar una vista de monitoreo de las tareas y su ejecución.
Centro de datos definido por software	La solución SDDC deberá permitir la adición de capacidades modulares opcionales, como automatización de la nube, además de la solución base. La solución deberá proveer la gestión para el conjunto (stack) completo de softwares integrado que agrupe en una sola plataforma la virtualización de cómputo, virtualización de almacenamiento, virtualización de red y la gestión de la nube. La solución deberá permitir crear y gestionar cargas de trabajo (dominios virtuales) de manera individual. Los dominios virtuales de cargas de trabajo en la solución SDDC deben estar controlados por políticas para proporcionar capacidad, disponibilidad y rendimiento específicos según lo requieran las cargas de trabajo.

### 1.2.1.7. Licenciamiento de Sistema Operativo

LICENCIAMIENTO DE SISTEMA OPERATIVO	
ATRIBUTOS	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Versión	El proveedor deberá incluir suscripciones de soporte de fabricante para el sistema operativo Red Hat Enterprise Linux for Virtual Datacenters versión 9 o superior con vigencia durante el tiempo de la garantía técnica.
Cantidad	El proveedor deberá incorporar las suscripciones necesarias para la cantidad de nodos hiperconvergentes solicitados en este documento. Estas suscripciones deberán permitir realizar la actualización a cualquier versión de Sistema Operativo superior estable que el fabricante del sistema operativo libere durante el periodo de vigencia de la suscripción. Adicionalmente, la suscripción deberá permitir la descarga del sistema operativo citado en este literal desde la página web del fabricante (portal web), descarga de parches de seguridad, reporte de incidentes en línea, acceso a actualizaciones, corrección de errores y asistencia técnica del fabricante del sistema operativo sin límite de número de incidencias reportadas bajo un esquema de atención de mínimo ocho (8) horas, los cinco (5) días de la semana los trescientos sesenta y cinco (365) días del año.
Administración	Se deberá incluir una solución de administración de sistemas que facilite la implementación, el escalado y la gestión de la infraestructura del sistema operativo Red Hat requerido en este apartado, en entornos físicos y virtuales. Esta herramienta de gestión deberá facilitar al Ministerio de Salud Pública el aprovisionamiento, la configuración y la actualización de los sistemas garantizando que su funcionamiento sea eficaz, seguro y cumpla con los diversos estándares. La solución de administración de gestión se deberá conectar directamente a Red Hat para descargar actualizaciones y sincronizar contenido, y además deberá ofrecer la flexibilidad de trabajar en un entorno

LICENCIAMIENTO DE SISTEMA OPERATIVO	
ATRIBUTOS	ESPECIFICACIONES TÉCNICAS SOLICITADAS
	<p>completamente desconectado. Las características mínimas de la solución deberán incluir lo siguiente:</p> <ul style="list-style-type: none"> <li>• Arquitectura multiempresa.</li> <li>• Control de acceso basado en funciones (RBAC) para usuarios y grupos con directorios externos.</li> <li>• Interfaz de usuario gráfica (GUI), interfaz de línea de comandos (CLI) e interfaces de programación de aplicaciones (API)</li> <li>• Administración de suscripciones avanzada.</li> </ul>
Licenciamiento	Todo licenciamiento/suscripción requerida en este documento de especificaciones, deberá ser registrado a nombre del Ministerio de Salud Pública.

### 1.2.1.8. Software de Orquestación de Respaldos

SOFTWARE DE ORQUESTACIÓN DE RESPALDOS	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Marco de análisis	El software ofertado deberá estar listado en el último diagrama de líderes del cuadrante mágico de Gartner para soluciones de software de recuperación y respaldo empresarial. El Oferente deberá adjuntar la documentación que sea pertinente que permita verificar lo solicitado en este apartado.
Marca	Especificar marca de la solución de respaldos
Versión	Deberá ser la última versión de software estable liberada por el fabricante del software de orquestación de respaldos. El proveedor deberá sustentar lo requerido en este apartado, con un certificado emitido por el fabricante del software de orquestación de respaldos.
Cantidad	400 licencias
Soporte	<p>La solución deberá proveer respaldos de ambientes de Shared Files o NAS desde cualquier sistema de archivos basados en NFS, SMB, Windows y Linux que permita el respaldo de archivos y export de bases de datos.</p> <p>La solución de software de orquestación de respaldos deberá incluir los componentes que permitan realizar el respaldo a nivel de archivos alojados dentro de las máquinas virtuales a ser desplegadas dentro de la infraestructura Hiperconvergente solicitada en este documento. Los sistemas operativos para considerar son: Centos 7.x o superior, Red Hat Enterprise Linux 7.x o superior. Así mismo deberá incluir los componentes que permitan realizar el respaldo a nivel de archivos alojados dentro de LPARs desplegadas sobre infraestructura Power IBM con sistemas operativos AIX versión 7.1 o superior.</p> <p>La solución de software de orquestación de respaldos no deberá necesitar de la instalación de agentes para poder realizar sus tareas de respaldo, recuperación y replicación de máquinas virtuales.</p> <p>La solución de software de orquestación de respaldos deberá permitir la programación de tareas de respaldo a cinta de los respaldos de máquinas virtuales obtenidos.</p> <p>La solución de software de orquestación de respaldos deberá permitir la restauración de bases de datos Oracle individuales, al servidor de origen o a un nuevo servidor Oracle. La solución deberá permitir la recuperación a nivel de transacción de bases de datos Oracle al mismo servidor o a uno diferente.</p> <p>La solución de software de orquestación de respaldos deberá permitir realizar respaldos sin detener las máquinas virtuales y sin generar degradación en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.</p> <p>La solución de software de orquestación de respaldos deberá permitir crear backups desde instantáneas (Snapshot's) de storage.</p> <p>La solución deberá permitir crear backups basados en imagen y réplicas con la frecuencia que establezca el Ministerio de Salud Pública con un impacto mínimo o nulo en el entorno de producción para backups, desde Snapshot's o instantáneas de los sistemas de almacenamiento primario y/o secundario.</p> <p>Deberá soportar las últimas versiones disponibles de los hipervisores, como mínimo VMware vSphere 6.5</p> <p>El software deberá presentar estadísticas de rendimiento, calendarización, trabajos, respaldos. Deberá permitir enviar alertas vía correo y SNMP.</p>

SOFTWARE DE ORQUESTACIÓN DE RESPALDOS	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Licenciamiento	Licenciamiento basado en instancias, de uso perpetuo, con servicio de mantenimiento y actualización del producto ofertado por el término mínimo estándar de la vigencia de la garantía técnica. Todo licenciamiento deberá ser registrado a nombre del Ministerio de Salud Pública. El proveedor deberá considerar la cantidad instancias instaladas en la solución de hiperconvergencia para el dimensionamiento del licenciamiento de la solución de orquestación de respaldos. La solución de software de orquestación de respaldos no deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.
Instalación y configuración	El proveedor deberá incluir la instalación y configuración de la solución ofertada (software de orquestación de respaldos requerida en este documento), con todas las funcionalidades incluidas dentro del producto ofertado y que determine el Ministerio de Salud Pública, dentro del equipo servidor detallado en este documento y conforme a las recomendaciones y buenas prácticas definidas por el fabricante del producto. Esta parametrización deberá incluir la configuración de los repositorios donde se realizarán los respaldos de las Máquinas Virtuales, así como de los repositorios para el respaldo de las bases de datos, repositorios NFS, las configuraciones de red, configuraciones del sistema operativo y demás prerrequisitos definidos por el fabricante del software de orquestación de respaldos y que permitan garantizar su rendimiento y funcionalidad.
Tareas de respaldo	El proveedor deberá incluir la configuración de mínimo ochenta (80) tareas de respaldo automatizadas para las máquinas virtuales que la DTIC determine y que se encontrarán desplegadas dentro de la solución Hiperconvergente requerida en este documento. El proveedor deberá ejecutar pruebas de generación y recuperación de los respaldos, con la finalidad de evidenciar el correcto funcionamiento de la solución y consistencia de los datos generados dentro del proceso de respaldo.
Integración con sistema de almacenamiento	La solución de software de orquestación de respaldos deberá ser integrada con la "solución de almacenamiento para respaldos" solicitada en este documento con la finalidad de mejorar el rendimiento en la ejecución de respaldos o recuperación. El proveedor deberá configurar dicha integración, aplicando las mejores prácticas determinadas por el fabricante de los equipos/software y los lineamientos que emita el Ministerio de Salud Pública.
Integración con bases de datos	La solución de software de orquestación de respaldos propuesta deberá incluir los componentes y/o funcionalidades necesarias para la ejecución de respaldos de instancias de base de datos Oracle a ser desplegadas en una infraestructura Power RISC con Sistema Operativo AIX 7.x o superior, operando sobre arquitectura Power RISC. La solución deberá tener integración con Oracle RMAN y deberá permitir una recuperación rápida a nivel de transacción de bases de datos a un punto preciso del tiempo y/o una transacción específica. Deberá permitir como mínimo lo siguiente: <ul style="list-style-type: none"> <li>Recuperación a nivel de transacciones a través del análisis del log de transacciones.</li> <li>Recuperación de bases de datos a un punto en el tiempo a través del replay del log de transacciones desde un backup de imagen en un solo paso.</li> <li>Gestionar logs archivados para evitar el llenado de backups y aprovechar al máximo la cantidad de almacenamiento usada para el backup.</li> <li>Recuperación en otra infraestructura de base de datos.</li> </ul> La solución de software de orquestación de respaldos deberá ser compatible con las bases de datos Oracle 12c, 19c o versión superior estable liberada por el fabricante a fecha de elaboración de este informe. PostgreSQL desde la versión 10.x hasta la última versión estable liberada por el fabricante a fecha de elaboración de este informe y MySQL desde la versión 5.3 hasta la última versión estable liberada por el fabricante a fecha de elaboración de este informe.
Respaldo y replicación	La solución de software de orquestación de respaldos deberá incluir funcionalidades de respaldo (backup) y replications integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada.
Cifrado y protección	La solución de software de orquestación de respaldos deberá permitir asegurar los datos de backup y las transferencias de red, con el cifrado end-to-end AES 256-bit o superior sin producir ningún impacto negativo en la compresión integrada y en la tasa de reducción de datos de la aceleración WAN. La solución deberá permitir asegurar los datos de backups y/o repositorios de backups contra ransomware.
Métodos de aceleración	Aceleración WAN incorporada. La solución de software de orquestación de respaldos deberá disponer de métodos de aceleración WAN incorporadas que permitan reducir el uso de ancho de banda en el traslado, ejecución o replica de respaldos a un sitio externo o remoto.
Transferencia de backups de base de datos	La solución de software de orquestación de respaldos deberá permitir transferir los backups de Oracle RMAN a los repositorios del software orquestador de respaldos y recuperar los mismos usando las funcionalidades de backup y restauraciones nativas de Oracle. La solución deberá soportar como mínimo motores de bases de datos Oracle instalados en sistemas operativos AIX.
Granularidad de respaldos	La solución de software de orquestación de respaldos deberá ser capaz de respaldar de forma indistinta, una máquina virtual completa o discos virtuales específicos de una máquina virtual.

SOFTWARE DE ORQUESTACIÓN DE RESPALDOS	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Herramienta de gestión de archivos	Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador.
Seguimiento de bloques de disco	La solución de software de orquestación de respaldos deberá permitir realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una replicación más frecuente.
Recuperación instantánea	La solución de software de orquestación de respaldos deberá permitir la recuperación instantánea de las máquinas virtuales, así mismo deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.
Proxy	La solución de software de orquestación de respaldos deberá permitir la agregación de servidores o multi dispositivos de respaldo en modo proxy de tal manera que la carga de procesamiento y tráfico de red que se generen dentro de la ejecución de las tareas de respaldo programadas, puedan ser distribuidas a través de estos servidores.
Latencia	La solución de software de orquestación de respaldos deberá permitir el establecimiento del nivel de latencia de E/S máximo aceptable para almacenes de datos de producción con la finalidad de garantizar que la copia de seguridad y las actividades de replicación, no afecten la disponibilidad del almacenamiento dedicado para las cargas de trabajo de producción.
Integración nativa con la librería robótica	La solución de software de orquestación de respaldos propuesta deberá tener integración nativa con la librería robótica solicitada en este documento. Adicionalmente deberá permitir la programación automática de tareas de respaldo a cintas LTO tanto de respaldos de máquinas virtuales como de archivos.
Pools de cintas LTO	La solución de software de orquestación de respaldos propuesta deberá permitir la creación de pools de cintas LTO con la finalidad de organizar la gestión de respaldos a dispositivos de este tipo. Adicionalmente deberá permitir definir pools con la siguiente política de retención de copias de seguridad en cinta mínima: <ul style="list-style-type: none"> <li>• Diario</li> <li>• Semanal</li> <li>• Mensual</li> <li>• Trimestral</li> <li>• Anual</li> </ul>
Restauración	La solución de software de orquestación de respaldos propuesta, luego de una recuperación rápida, deberá poder realizar una restauración total sin interrupciones del servicio. La solución deberá permitir que el trabajo realizado por los usuarios no se vea afectado al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción. La solución de software de orquestación de respaldos propuesta deberá permitir la restauración y reinicio de una máquina virtual respaldada, directamente desde su backup alojado en el sistema de almacenamiento deduplicado. La solución de software de orquestación de respaldos propuesta deberá proveer la capacidad de completar restauraciones completas del respaldo (backup) de cualquier máquina virtual dentro de una ventana de mantenimiento mínima. La estrategia deber consistir en replicar o realizar una copia en caliente del respaldo (backup) de la máquina virtual que se encuentra en un almacenamiento deduplicado, al almacenamiento en producción donde la máquina virtual se ejecuta.
Recuperabilidad e integridad	La solución de software de orquestación de respaldos deberá permitir verificar automáticamente la recuperabilidad/integridad de los backups generados.
Orquestación	La solución de software de orquestación de respaldos deberá soportar la generación de mínimo: Informes de vistas generales de configuraciones de la solución de software de orquestación de respaldos, auditorías de la infraestructura de backups, informes de cumplimiento, máquinas virtuales protegidas (VM), Capacity Planning, e informes de cintas.
Consola de Administración	La solución de software de orquestación de respaldos deberá incluir una consola de administración instalable incluso en un equipo de cliente y que permita administrar (localmente desde el servidor donde se encuentre instalado el software de orquestación de respaldos o remotamente desde un equipo de un cliente) las tareas de respaldo, administrar los repositorios, las unidades de respaldo a cinta, y en general administrar todas las funcionalidades del software de orquestación de respaldos requerido en este documento. Adicionalmente deberá incluir funcionalidades de reportería y alertas centralizadas. La solución deberá permitir centralizar la administración de varios servidores de respaldo en un único panel de control o consola de administración.
Replicación	La funcionalidad de replicación de máquinas virtuales deberá permitir el establecimiento de políticas de replicación con un RPO parametrizable desde cinco (5) minutos mínimos hasta veinticuatro (24) horas, configurable para cada máquina virtual individual.

## 1.2.2. Equipos de conectividad

En las especificaciones técnicas de los equipos de conectividad se hará referencia a los siguientes subcomponentes:

- Switches LAN para Integración de Sistema Hiperconvergente.
- Switches LAN para Red de Administración.

### 1.2.2.1. Switches LAN para Integración de Sistema Hiperconvergente

SWITCHES LAN PARA INTEGRACIÓN DE SISTEMA HIPERCONVERGENTE	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Marca	Especificar.
Modelo	Especificar.
Tipo	Deberá ser catalogado como switch para data center, lo cual deberá estar publicado en la página web oficial del fabricante, así como en datasheet del producto. Adjuntar certificado del fabricante que avale lo solicitado.
Cantidad	Se deberá incluir dos (2) switches LAN para la comunicación redundante de los nodos hiperconvergentes.
Fabricación	Deberán ser de fabricación de mínimo año 2024 o superior, nuevos de fábrica, no remanufacturados, ni reparados en ninguna de sus partes. Los equipos ofertados no deberán estar listados como "End of Sale" y "End of Support" por el fabricante, a fecha de firma de acta entrega recepción de equipos. El proveedor deberá sustentar lo requerido en este apartado, con un certificado emitido por el fabricante.
Generación de fabricación:	La última generación de equipos disponible por el fabricante para el modelo de Switchs LAN ofertados. El proveedor deberá incluir un certificado emitido por el fabricante de los equipos Switchs LAN ofertados que permita avalar lo solicitado en este apartado.
Formato	Hasta dos (2) unidades de Rack cada Switch LAN.
Capacidad	<p>Cada switch LAN para integración deberá ser capaz de operar en capa 2 (L2) y capa 3 (L3). Cada switch LAN para integración deberá incluir como mínimo los siguientes puertos:</p> <ul style="list-style-type: none"> <li>• 48 puertos 10/25 Gbps. Licenciados para poder trabajar a todas estas velocidades.</li> <li>• 6 puertos 100 Gbps. Licenciados para poder trabajar a todas estas velocidades.</li> </ul> <p>Cada switch LAN para integración deberá incluir como mínimo los siguientes Transceivers y/o cables Direct Attach y/o elementos de conectividad necesarios para las conexiones requeridas:</p> <ul style="list-style-type: none"> <li>• Dos (2) transceivers QSFP28-DD capaces de operar a 200 Gbps, requeridos para la configuración de HA (alta disponibilidad).</li> <li>• Dos (2) transceivers QSFP28 capaces de operar a 100 Gbps, requeridos para la conexión en HA (alta disponibilidad) con los switches de administración.</li> <li>• Catorce (14) transceivers SFP28, para la interconexión con los nodos hiperconvergentes a 25Gbps.</li> <li>• Seis (6) transceivers SFP28 capaces de operar a velocidades de 25Gbps para conexión del servidor de respaldo y el almacenamiento de respaldos requeridos en este documento.</li> <li>• Diez (10) transceivers SFP+ capaces de operar a velocidades de 10Gbps para integración con los servidores IBM Power nuevos, chassis Blade IBM FlexSystem.</li> <li>• Cada switch LAN para integración deberá incluir los cables necesarios, de mínimo un metro de longitud con soporte para velocidad de mínimo 200Gbps para configuración de alta disponibilidad.</li> </ul> <p>El proveedor deberá incluir los elementos y/o conectores y/o cables y/o PatchCords necesarios para conectar todos los nodos de hiperconvergencia y sistema de gestión de respaldos, solicitados en este documento, de forma redundante, a cada uno de los puertos de 25GbE SFP28 solicitados en cada nodo Hiperconvergente, puertos del sistema de gestión de respaldo y puertos de infraestructura existente; así como para la interconexión a mínimo 200Gbps entre switches para la alta disponibilidad requerida. Cada switch deberá soportar características de networking para hacer cascada, agregación de enlaces (link aggregation), calidad de servicio (QoS) y seguridad.</p>

SWITCHES LAN PARA INTEGRACIÓN DE SISTEMA HIPERCONVERGENTE	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Switching Capacity	Cada switch tendrá una capacidad de switching de mínimo 2 Tbps.
Throughput	Cada switch tendrá un Throughput de mínimo 2000 Mpps
Puertos de consola	Puertos de consola por switch: Como mínimo uno (1) RJ45
Alta disponibilidad	Se deberá configurar los dos equipos en Alta Disponibilidad en funcionamiento Activo-Activo
Ventilación	Los ventiladores deberán ser redundantes
Puertos de acceso	Todos los puertos de acceso Ethernet deberán funcionar a tasas completas (full rate ó Line rate non-blocking).
Alimentación de poder	Alimentación de 100 a 240V AC 60Hz. Deberán incluir fuentes de energía redundantes y los cables de alimentación eléctrica para los tomacorrientes con líneas a tierra. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC320-C14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del Ministerio de Salud Pública.
Actualización de firmwares	El sistema operativo de los switches deberá soportar la funcionalidad de actualización en caliente o realizar actualización de uno de los sistemas y el segundo soportar toda la carga y viceversa con mínima pérdida durante la misma.
Protocolos	Cada switch deberá soportar protocolos de capa 3 como OSPF, BGP y Vxlan en capa 2.

### 1.2.2.2. Switches LAN para Red de Administración

SWITCHES LAN PARA RED DE ADMINISTRACIÓN	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Marca	De la misma marca del fabricante de los switches Switches LAN para Integración del Sistema Hiperconvergente y sistema de gestión de respaldos ofertados.
Modelo	Especificar
Cantidad	Se deberá incluir dos (2) switches LAN para la comunicación redundante de la red de administración de todos los equipos ofertados.
Fabricación	Deberán ser de fabricación de mínimo año 2024 o superior, nuevos de fábrica, no remanufacturados, ni reparados en ninguna de sus partes. Los equipos ofertados no deberán estar listados como "End of Sale" y "End of Support" por el fabricante, a fecha de firma de acta entrega recepción de equipos. El proveedor deberá sustentar lo requerido en este apartado, con un certificado emitido por el fabricante.
Generación de fabricación:	La última generación de equipos disponible por el fabricante para el modelo de Switchs LAN ofertados. El proveedor deberá incluir un certificado emitido por el fabricante de los equipos Switchs LAN ofertados que permita avalar lo solicitado en este apartado.
Formato	Una (1) unidad de Rack cada Switch LAN.
Capacidad	<p>Cada switch LAN para red de administración deberá ser capaz de operar en capa 2 (L2) y capa 3 (L3).</p> <p>Cada switch LAN para red de administración deberá incluir como mínimo los siguientes puertos:</p> <ul style="list-style-type: none"> <li>• 48 puertos multi-gigabit 100M/1000M/2.5Gb/5G/10G BaseT Ethernet</li> <li>• Puertos de Uplink: <ul style="list-style-type: none"> <li>○ 4 puertos 10/25Gbps SFP28</li> <li>○ 2 puertos 40/100Gbps QSFP28</li> </ul> </li> </ul> <p>Cada switch LAN para Red de Administración deberá incluir como mínimo los siguientes Transceivers y/o cables Direct Attach y/o elementos de conectividad necesarios para las conexiones requeridas:</p> <ul style="list-style-type: none"> <li>• Dos (2) transceivers SFP28 capaces de operar a velocidades de 25 Gbps, requeridos para la configuración de HA (alta disponibilidad).</li> <li>• Dos (2) transceivers QSFP28 capaces de operar a velocidades de 100 Gbps, requeridos para la conexión uplink a los switches de interconexión</li> </ul>

<b>SWITCHES LAN PARA RED DE ADMINISTRACIÓN</b>	
<b>ATRIBUTO</b>	<b>ESPECIFICACIONES TÉCNICAS SOLICITADAS</b>
	<ul style="list-style-type: none"> <li>24 puertos licenciados para soportar velocidades de 100M/1000M/2.5Gb/5G/10G Base-T para conexión al "core" de CNT EP, proveedor del servicio de Housing y Comunicaciones del Ministerio de Salud Pública, dos servidores IBM Power 7 existentes, almacenamiento IBM nuevo y servidores DELL EMC PowerEdge Gen14 y Gen15 existentes</li> <li>24 puertos licenciados para soportar velocidades de 100M/1000M Base-T para conexión de los puertos de administración del sistema hiperconvergente, servidor y almacenamiento para respaldo.</li> </ul> <p>El proveedor deberá incluir los accesorios y/o conectores y/o cables (Patch Cords) necesarios para conectar todos los puertos de administración de los nodos de hiperconvergencia y equipos para respaldo solicitados además de la infraestructura existente. Cada switch deberá soportar características de networking para hacer cascada, agregación de enlaces (link aggregation), calidad de servicio (QoS) y seguridad.</p>
Switching Capacity	Cada switch tendrá una capacidad de switching non-blocking de mínimo 1.5Tbps.
Throughput	Cada switch tendrá un Throughput de mínimo 490 Mpps.
Puertos de consola	Como mínimo uno (1) RJ45
Alta disponibilidad	Se deberá configurar los dos equipos en Alta Disponibilidad en funcionamiento Activo-Activo
Ventilación	Especificar.
Puertos de acceso	Todos los puertos de acceso Ethernet (downlink) deberán funcionar a tasas completas (full rate ó Line rate non-blocking).
Alimentación de poder	Alimentación de 100 a 240V AC 60Hz. Deberán incluir los cables de alimentación eléctrica para los tomacorrientes con líneas a tierra. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC320-C14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del Ministerio de Salud Pública.

### 1.2.3. Solución de Almacenamiento para Respaldos

<b>SOLUCIÓN DE ALMACENAMIENTO DE RESPALDOS</b>	
<b>ATRIBUTO</b>	<b>ESPECIFICACIONES TÉCNICAS SOLICITADAS</b>
Cantidad	Uno
Marca	Especificar.
Generación de fabricación	La última generación de equipos disponible por el fabricante para el modelo ofertado. El proveedor deberá incluir un certificado emitido por el fabricante de los equipos que permita avalar lo solicitado en este apartado.
Formato	El dispositivo deberá permitir realizar el respaldo y recuperación de información basado en discos duros, mediante un mecanismo de optimización de deduplicación; dicha deduplicación deberá de realizarse en línea, durante la ingesta de los datos.
Tipo	La solución deberá ser un sistema de almacenamiento basada en un equipo appliance con propósito específico para respaldos con características de altos niveles de deduplicación y compresión, no se aceptarán sistemas de almacenamiento SAN y/o NAS de propósito general o para otros propósitos específicos. El proveedor deberá incluir DataSheet público del producto y un certificado emitido por el fabricante de los equipos que permita avalar lo solicitado en este apartado.
Licenciamiento	El sistema deberá incluir el licenciamiento de funcionalidad de deduplicación y compresión de los bloques de los datos de los respaldos para toda la capacidad de almacenamiento requerida en esta especificación técnica. La deduplicación se define como la funcionalidad que permite la eliminación de segmentos redundantes con el fin de aprovechar de manera óptima la capacidad de almacenamiento.
Protección de datos	El sistema deberá soportar la falla simultánea de hasta dos discos, el arreglo deberá contar con protección de hardware RAID-6 o similar.
Monitoreo	El software deberá presentar estadísticas de rendimiento y ahorros debido a la compresión y deduplicación, deberá permitir enviar alertas vía correo y SNMP.
Protocolos:	Deberá soportar los protocolos CIFS y NFS para presentar volúmenes y realizar respaldos por LAN. También debe soportar protocolo de conectividad Fibre Channel o emulación VTL sobre Fibre Channel.



SOLUCIÓN DE ALMACENAMIENTO DE RESPALDOS	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
Capacidad requerida	El dispositivo deberá suministrarse con la capacidad útil de mínimo 150TB, antes de compresión y deduplicación, después de RAID y formato; de la cual está considerado la utilización de máximo el 80% (120TB) para no degradar el rendimiento. Cada proveedor deberá considerar como capacidad a no ser utilizada, mínimo 20% de la capacidad ofertada, según la mejor practica que determine el fabricante, para no degradar el rendimiento del dispositivo; debidamente licenciados y considerando como mínimo la configuración de protección RAID-6 o similar.
Capacidad de Crecimiento	Como mínimo a 450TB usables.
Almacenamiento	<p><b>1.- Híbrido:</b> En esta configuración el equipo deberá tener las siguientes características y configuraciones mínimas:  <b>Boot:</b> Debe bootear desde dispositivos SSD, estos dispositivos pueden ser los discos SSD de cache/metadata o discos adicionales para uso específico de Boot.            Cache/Metadata: Mínimo 5 discos SSD de mínimo 3.84TB con la finalidad de garantizar el rendimiento de escritura/lectura de datos.            La capacidad útil para datos requerida deberá ser configurada con discos de mínimo tipo SAS o NL-SAS 7.2K RPM de mínimo 8TB</p> <p><b>2.- Todo Flash:</b> En esta configuración el equipo deberá tener las siguientes características y configuraciones mínimas:  <b>Boot:</b> A través de disco de uso específico para boot o dispositivos flash de la capacidad util.            Cache/Metadata: No requerido por ser todo flash            La capacidad útil para datos requerida deberá ser configurada con dispositivos flash de la menos 7,68TB.</p>
Compatibilidad	Deberá ser compatible con software de orquestación de respaldos solicitado en esta especificación técnica.
Conectividad	La solución propuesta deberá contar con mínimo cuatro (4) puertos de mínimo 16 Gbps FC HBA LC-LC para integración con la red SAN, mínimo un (1) puerto Ethernet de 1Gbps para administración del equipo y mínimo cuatro (4) puertos 25 Gbps SFP+ con conector LC-LC para integración con los switches de integración del sistema hiperconvergente. Deberá incluir todos los transceivers que sean requeridos para las tecnologías y cantidad de puertos solicitados en este apartado y en general para todos los demás puertos que se incluyan como parte del equipo.
Disponibilidad	El dispositivo deberá incluir fuentes de poder y ventiladores redundantes y reemplazables en caliente.
Rendimiento	Ancho de banda de respaldo físico del sistema: Mínimo 30TB/hora.
Mecanismos de Protección de Información	El proveedor deberá incluir mínimo un repuesto en caliente por cada Grupo RAID o por cada Enclosure de discos para la arquitectura y configuración ofertada, independiente de los discos requeridos para suministrar la capacidad solicitada.
Protección:	La solución propuesta deberá contar con el nivel de protección en RAID 6 o similar/superior, dicho RAID se deberá de realizar a nivel de hardware y no vía software.
De-Duplicación de datos	La solución propuesta deberá incluir la funcionalidad de deduplicacion. La deduplicacion deberá efectuarse en línea, durante la ingesta de datos a fin de minimizar los requisitos de disco para respaldo y archiving. La relación de reducción de datos de la deduplicación de la solución deberá ser de mínimo hasta 50:1, respaldada con información que conste en el DataSheet público del producto ofertado y carta emitida por el fabricante de la marca ofertada que avale este requerimiento.
Inmutabilidad	El dispositivo deberá incorporar mecanismos de inmutabilidad para protección en el acceso a los datos, borrados y modificaciones, los cuales deben ser detallados en la oferta. Se deberá incluir el licenciamiento necesario para estas características.
Administración	El dispositivo deberá contar con un software de gestión propio que permita su administración vía GUI o Web. Deberá tener la capacidad de generar y enviar correos electrónicos o alarmas a una consola de gestión y soporte de SNMP Traps. Deberá permitir exportar información de monitoreo, log de errores, etc. hacia "fuera" del dispositivo.
Servicios de notificación de eventos	El arreglo de discos y/o equipo ofertado deberá contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos de falla hacia el centro de soporte del fabricante.
Fuente de poder y	El equipo de almacenamiento deberá incluir fuentes de poder y ventiladores 100-240 VAC redundantes y hot-swap. El tipo de conector de los cables de interconexión eléctrica (terminal que

SOLUCIÓN DE ALMACENAMIENTO DE RESPALDOS	
ATRIBUTO	ESPECIFICACIONES TÉCNICAS SOLICITADAS
ventiladores	se conectará a la PDU del Rack) deberán ser de tipo IEC320-C14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del Ministerio de Salud Pública.
Cables de poder y adicionales	El proveedor deberá incluir todos los cables eléctricos que permitan la interconexión eléctrica de toda la solución ofertada y de manera redundante. Adicionalmente deberá incluir los rieles de montaje para rack estándar de centro de datos.
Consola o interfaz web de administración	El equipo de almacenamiento se deberá entregar con licenciamiento de tipo perpetuo y a nombre del Ministerio de Salud Pública. Deberá permitir la administración de la solución ofertada, desde una consola (interfaz gráfica) o desde un browser, para toda la capacidad requerida. Protocolos Web-based GUI; SSH CLI; SMI-S; SNMP
Administración, monitoreo y estadísticas de desempeño	El software de administración del equipo de almacenamiento ofertado deberá: dotar de estadísticas para un rápido diagnóstico, solución de problemas y optimización de la carga. Visualizar en tiempo real el desempeño de I/O tanto en escritura como de lectura. Visualizar en tiempo real el uso de: CPU, sistema cache, discos, red y volúmenes, soporte de SMI-S y soporte de protocolo SNMP.

## 2. GARANTÍA TÉCNICA

Detalle de la Garantía Técnica que aplica para todos los componentes que conforman esta solución			
Tipo	Tiempo	Detalle	Observación
Garantía Técnica	5 años	Mantenimiento preventivo. El proveedor deberá realizar, dos (2) visitas al año para ejecuciones de mantenimiento preventivo y limpieza del equipamiento requerido, esto en coordinación con la Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública.	El mantenimiento preventivo durante los cinco (5) años NO tendrá costo para el Ministerio de Salud Pública.
		Mantenimiento correctivo. Es parte de la Garantía Técnica la reparación inmediata del bien en caso de daño o defecto de funcionamiento, la provisión e instalación de repuestos, accesorios, piezas o partes.	El mantenimiento correctivo durante el tiempo de la Garantía Técnica, NO tendrá costo para el Ministerio de Salud Pública.
		Reemplazo de los bienes por daños de fábrica. Contempla el reemplazo de los bienes por daño de fábrica y provisión del o los equipos con iguales o superiores características mientras se realiza el reemplazo respectivo.	El Reemplazo de los bienes por daños de fábrica durante el tiempo de la Garantía Técnica, NO tendrá costo para el Ministerio de Salud Pública.
		Horas de Soporte	Horas de Soporte, durante el tiempo de la Garantía Técnica, NO tendrán costo para el Ministerio de Salud Pública, el SLA respectivo se regirá de acuerdo a los "Servicios de Horas de Soporte".
		Soporte fabricante	Soporte fabricante, durante el tiempo de la Garantía Técnica, NO tendrá costo para el Ministerio de Salud Pública.

### 2.1. NIVELES DE SERVICIO (SLA) DE TODOS LOS COMPONENTES QUE FORMAN PARTE DE LA SOLUCIÓN

NIVELES DE SERVICIOS (SLA)
Todo el hardware, software (incluido el software de virtualización, sus componentes de almacenamiento y en general todo componente de software que permite su funcionamiento) y firmware que conforman la solución requerida en estas especificaciones técnicas, deberán disponer de una garantía técnica, soporte y suscripción de sus fabricantes vigente durante el tiempo de la garantía en modalidad 24x7x365.

El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante, o por medio del contratista. En cualquiera de los casos, el Ministerio de Salud Pública se reserva el derecho de definir la prioridad de un evento/incidente de servicio de soporte.

El contratista deberá disponer de una mesa de servicios para gestionar la atención de incidencias sobre el hardware adquirido.

El contratista deberá poner a disposición el Administrador de Contrato designado por el Ministerio de Salud Pública lo siguiente: El procedimiento y mecanismos de apertura, categorización, seguimiento y escalamiento de casos, el cual deberá entregarse en un plazo máximo de 5 días laborables posterior a la firma del acta entrega recepción de los bienes.

La garantía técnica de fabricante deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo seis (6) horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El contratista se encargará de tramitar cualquier cambio de partes (RMA - Return Merchandise Authorization) ante el fabricante y de acuerdo con el SLA que se detalla más adelante.

El contratista deberá entregar un informe de cada caso o incidente reportado, el cual como mínimo deberá contener:

- Descripción del caso/incidente
- Identificación del Problema
- Acciones tomadas
- Recomendaciones
- Fecha y hora de inicio
- Fecha y hora fin
- Comunicaciones indicadas por el fabricante para la solución del caso
- Posibles detecciones de problemas que deben estudiarse y/o resolverse con un cambio de hardware

El informe se lo entregará una vez completada la atención dentro de las siguientes dieciséis (16) horas laborables, concluyendo con este informe los casos reportados. Al finalizar cada trimestre, dentro de los siguientes ocho (8) días laborables, el contratista deberá entregar un reporte consolidado de casos atendidos. El primer trimestre empieza en la fecha de firma del acta entrega recepción definitiva de los bienes.

Los servicios de soporte de fábrica del sistema hiperconvergente deberán ser entregados en forma unificada por el fabricante de los equipos: hardware de los nodos, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión a través de un servicio de soporte integral y unificado. El contratista deberá adjuntar un certificado emitido por el fabricante de los equipos que avale lo solicitado en este apartado.

**NIVELES DE SERVICIO (SLA) PARA SOPORTE Y MANTENIMIENTO**

Prioridad	Descripción	Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente	Modalidad de comunicación	Tiempo máximo de diagnóstico del incidente o problema	Forma de Trabajo, para diagnóstico o solución	Tiempo máximo de Cambio de Repuestos y solución a incidentes.
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con el contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	6 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública
Media	Herramienta continúa en funcionamiento causa molestias, pero no se paralizará la producción en el corto plazo	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con el contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	12 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública

Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta minutos (60)	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con el contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública
------	--	----------------------	--	--	--	---

## 2.2. NIVELES DE SERVICIO (SLA) DE HORAS DE SOPORTE

Servicios de Horas de Soporte			
Cantidad	200 horas		
El contratista, como parte de la solución, proporcionará un pool horas de soporte mientras dure la garantía técnica. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adición de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública relacionado a la administración y operación/reconfiguración de la solución de respaldos detallada en este documento. Se establecen los siguientes horarios de soporte (SLA), el cual estará disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5x365 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará bajo el siguiente detalle:			
Prioridad	Descripción	Tiempo Respuesta para iniciar trabajos de soporte	Tipo Soporte
Alta	Se requiere del soporte para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.	Hasta 2 horas luego de la solicitud de soporte realizada por el MSP	Remoto y/o Teléfono
		Hasta 5 horas luego de la solicitud de soporte realizada por el MSP	En sitio, Remoto o Telefónico
Moderada	Se requiere del soporte canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	Hasta 7 horas luego de la solicitud de soporte realizada por el MSP	En sitio, Remoto o Telefónico
Baja	Se requiere de soporte canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas luego de la solicitud de soporte realizada por el MSP	En sitio, Remoto o Telefónico
Esquema de horarios de atención y consumo de horas de soporte:	<ul style="list-style-type: none"> <li>Las horas de soporte ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.</li> <li>Las horas de soporte ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.</li> <li>Las horas de soporte ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.</li> <li>Las horas de soporte ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.</li> <li>Para el registro del consumo y utilización de las horas de soporte canal, se contabilizará las horas/minutos efectivamente utilizados dentro de las actividades de soporte requeridas por el Ministerio de Salud Pública y ejecutadas por el contratista.</li> </ul>		

### 3. MANUALES TÉCNICOS

Los manuales, catálogos, hojas técnicas de los equipos solicitados, deberán ser entregados como parte de la oferta, así como también al momento de la instalación y puesta en funcionamiento de los equipos.

Los manuales deberán ser entregados por parte del oferente adjudicado en forma impreso o digital, de preferencia en idioma español o inglés.

### 4. MODALIDAD DE CAPACITACIÓN

El contratista efectuará la capacitación al personal respectivo de la DTIC, bajo el siguiente detalle:

MODALIDAD DE CAPACITACIÓN			
La capacitación se deberá organizar en mínimo dos (2) grupos de mínimo siete (7) funcionarios por cada grupo.			
Los horarios, la modalidad de asistencia de los grupos y el personal a asistir serán coordinados con la Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública.			
La capacitación deberá ser orientada en la configuración y uso/administración en todas las funcionalidades o features de la solución contratada.			
La capacitación será de forma presencial en las instalaciones autorizadas del contratista adjudicado.			
El material utilizado deberá ser oficial de la marca de la solución, además, deberá ser entregado impreso o en formato digital a los participantes que asistan a la capacitación.			
El contratista adjudicado previamente al desarrollo de esta actividad deberá presentar el plan y temario de capacitación en formato digital para que sea revisado y aprobado por el administrador del contrato.			
El contratista adjudicado deberá proveer todos los equipos y las máquinas virtuales necesarios para la capacitación en un escenario lo más cercano a la implementación a realizarse.			
Se deberá entregar por parte del contratista un informe detallado, de los temas impartidos en la capacitación con número de horas.			
Al cumplimiento de la capacitación se deberá entregar los certificados de aprobación a los funcionarios del Ministerio de Salud Pública.			
El Ministerio de Salud Pública se reserva el derecho de la reorganización de horas de capacitación previa coordinación con el contratista.			
La capacitación deberá ser realizada como mínimo de acuerdo al siguiente esquema, el contratista deberá considerar que existirá el aumento de horas de acuerdo a la complejidad de la solución contratada.			
Componentes de la solución integral	Tema	Horas por grupo	Cantidad total de horas de capacitación por componente
Componente 1	Sistema Hiperconvergente	12	228 horas Mínimo dos (2) grupos de mínimo siete (7) funcionarios por cada grupo.
	Nodos Hiperconvergentes	16	
	Virtualización de Cómputo	12	
	Virtualización Almacenamiento	12	
	Gestión Virtualización	12	
	Gestión de Seguridad	10	
	Gestión del Ciclo de Vida	10	
	Licenciamiento de Sistema Operativo	10	
Software de Orquestación de respaldos	20		
<b>Total horas por grupo, Componente 1</b>		<b>114</b>	

<b>Componente 2</b>	Switches LAN para Integración de Sistema Hiperconvergente	6	24 horas Mínimo dos (2) grupos de mínimo siete (7) funcionarios por cada grupo.
	Switches LAN para Red de Administración	6	
<b>Total horas por grupo, Componente 2</b>		<b>12</b>	
<b>Componente 3</b>	Solución de almacenamiento de respaldos	14	28 horas Mínimo dos (2) grupos de mínimo siete (7) funcionarios por cada grupo.
	<b>Total horas por grupo, Componente 3</b>		
<b>Total horas por grupo</b>		<b>140 horas</b>	
<b>Total de horas de capacitación</b>			<b>280 horas</b> <b>Mínimo dos (2) grupos de mínimo siete (7) funcionarios por cada grupo.</b>

## 5. METODOLOGÍA DE TRABAJO

Una vez suscrito el contrato el contratista contemplará y realizará:

ITEM	METODOLOGÍA DE TRABAJO
1	El contratista deberá coordinar los trabajos de adecuación de cableado estructurado con el/los contratistas autorizados de la Corporación Nacional de Telecomunicaciones CNT E.P y el Ministerio de Salud Pública.
2	El contratista deberá incluir todos los cables eléctricos que permitan la integración de la solución a la red eléctrica de manera redundante. Adicionalmente deberá incluir los rieles de montaje para rack estándar del centro de datos para todos los equipos que forman parte de su solución.
3	El contratista deberá entregar un cronograma y plan de entrega para la instalación, configuración y puesta en marcha de los equipos y movimiento de las máquinas virtuales en el centro de datos de CNT EP., en coordinación con el administrador de contrato.
4	El contratista deberá entregar un cronograma y plan para realizar el mantenimiento preventivo de los equipos, durante el periodo de garantía técnica.
5	El contratista deberá entregar un plan de capacitación al administrador del contrato que contemple a los técnicos delegados por el Ministerio de Salud Pública.
6	El contratista deberá contemplar que la solución, en su totalidad, deberá ser diseñada, armada, configurada, instalada y probada por el contratista con sus ingenieros certificados por el fabricante del sistema hiperconvergente ofertado o con servicios directos del fabricante del sistema hiperconvergente ofertado, con base a las mejores prácticas de diseño e implementación para este tipo de arquitecturas que determinen tanto el contratista y/o fabricante en todos los componentes requeridos. La instalación será bajo supervisión, responsabilidad y participación del contratista.
7	El contratista deberá incluir todo el hardware y software requerido para el correcto funcionamiento del sistema hiperconvergente.
8	El contratista deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución, en forma detallada y a manera de procedimiento técnico documentado. Este manual técnico deberá permitir la reinstalación de cualquier componente de hardware y/o software que conforman la solución contratada.
9	El contratista desarrollará un Plan del Proyecto con rutas críticas, eventos e hitos, este plan deberá ser elaborado con la coordinación y lineamientos emitidos por personal técnico del Ministerio de Salud Pública, en este documento se reflejarán los requerimientos técnicos del Ministerio de Salud Pública para todos los componentes de la solución, de acuerdo con el diseño establecido por la institución y las mejores prácticas determinadas por el/los fabricante(s) para este tipo de despliegues.
10	El contratista deberá incluir todos los catálogos de los equipos ofertados en formato impreso o digital de preferencia en idioma español o inglés.
11	El contratista deberá entregar e instalar todo el equipamiento requerido por el Ministerio de Salud Pública en su centro de datos ubicado en las instalaciones del Mega Centro de Datos de la Corporación Nacional de Telecomunicaciones CNT E.P., ubicado en el sector de La Armenia, bajo coordinación del personal técnico de la Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública.

ITEM	METODOLOGÍA DE TRABAJO
12	En todos los casos, el contratista deberá considerar los lineamientos técnicos y estándares que disponga y exija la Corporación Nacional de Telecomunicaciones CNT E.P., para la instalación de cableado estructurado en racks de servidores y comunicaciones dentro del Mega Centro de Datos - la Armenia, así como los patch panels, conectores, patch cords y demás componentes requeridos.
13	El contratista deberá instalar la solución, de acuerdo con las necesidades de diseño de "Arquitectura propuesta" del Ministerio de Salud Pública, y deberá considerar todos los componentes necesarios de adecuación en los racks para la interconexión (Fibra, Cobre, San, Reflejos) siendo estos en un esquema de alta disponibilidad y tomando en consideración que la instalación será dentro del centro de datos del Ministerio de Salud Pública, ubicado en el Mega Centro de Datos de la Corporación Nacional de Telecomunicaciones CNT E.P., con la finalidad de permitir la integración de todos los equipos requeridos.
14	La ubicación final de cada reflejo en los racks del Ministerio de Salud Pública, puede variar de acuerdo al diseño que se aplique, sin embargo, el contratista deberá considerar que la distancia máxima entre racks no superará los 15 metros lineales. En todos los casos, el contratista podrá realizar inspecciones al centro de datos con la finalidad de establecer la arquitectura a implementar.
15	La longitud de los cables deberá ser la adecuada para permitir una organización y peinado eficientes en cada rack, se deberá garantizar el radio de curvatura indicado en las especificaciones técnicas de los cables. El contratista deberá incluir los organizadores de cableado horizontales que se requieran, con la finalidad de facilitar el peinado y organización del cableado estructurado requerido.
16	El contratista deberá etiquetar y peinar todo el cableado de FO y Cobre solicitado en la solución, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo con los lineamientos de la Corporación Nacional de Telecomunicaciones y la DTIC. Todo el cableado de FO y Cobre que el contratista instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes. Las adecuaciones a ser efectuadas por parte del contratista deberán ser estandarizadas de acuerdo a los lineamientos del documento denominado "Requerimientos Mínimos de Cableado en los CTIs" y ejecutadas por los contratistas certificados por parte de la Corporación Nacional de Telecomunicaciones CNT E.P.
17	Durante la ejecución del contrato el contratista coordinará con el administrador de contrato, todas las actividades de entrega, implementación y movimiento de las máquinas virtuales y puesta en marcha de los equipos y demás actividades concernientes a la ejecución del contrato.

## 6. OTROS PARÁMETROS REQUERIDOS POR LA ENTIDAD

Certificado de Distribuidor Autorizado, fabricante, representante, distribuidor o vendedor autorizado	El oferente deberá entregar adjunto con su propuesta los certificados que demuestren su condición de distribuidor o vendedor autorizado, fabricante, representante de las marcas correspondientes a los productos de hardware y software ofertados. Estos certificados deberán ser emitidos directamente por los fabricantes de los equipos ofertados y contar con una fecha de emisión del año 2024 o superior.
---	--