INFRAESTRUCTURA DE SERVIDORES EN HIPERCONVERGENCIA Y SERVIDOR DE COPIAS O BACKUPS

No. JEMPP - CEDE6-DIPCO-ET-05692-COM-00



INFRAESTRUCTURA DE SERVIDORES EN HIPERCONVERGENCIA Y SERVIDOR DE COPIAS DE SEGURIDAD O BACKUPS No. JEMPP - CEDE6-DIPCO-ET-05692-COM-00

CONTENIDO

1. OBJETO 3
2. DEFINICIONES Y APLICACIÓN 3
3. REQUISITOS 4
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 17
5. MÉTODOS DE ENSAYO 17
6. APÉNDICE 20
7. ANEXOS 22
8. CONTROL DE REVISIONES 22

Elaboró	Revisó	Aprobó
TO. JUN CARLOS SUÁREZ Comité Técnico Estructurador TIC-B6 ESMIC	**CT. LAURA KARINA PINEDA MIRANDA** Oficial B11 ESMIC	**CR. GEOVANNI ANDRÉS CORTÉS MOLINA** Subdirector ESMIC

1. OBJETO

Establecer los requisitos técnicos para una INFRAESTRUCTURA DE SERVIDORES EN HIPERCONVERGENCIA Y SERVIDOR DE COPIAS O BACKUP.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

- **Almacenamiento de Datos:** El almacenamiento de datos es el proceso tecnológico donde se graban, archivan y guardan bits de información que contienen imágenes, texto, video, programas, hojas de cálculo, entre otros archivos digitales de múltiples formatos. Existen diversas arquitecturas y dispositivos de almacenamiento para cumplir este propósito.

- **Backup:** Un sistema de backup, también conocido como copia de seguridad, reserva una copia de los datos y los almacena en un lugar seguro, ya sea una unidad física (disco duro) o en la nube (en un servidor de almacenamiento de internet como, por ejemplo, Google Drive). La copia de seguridad permite acceder a los datos siempre y cuando quieras, incluso recuperarlos en el caso de la pérdida de archivos originales.

- **Hiperconvergencia:** Plataforma de servidor virtualizado preconfigurado que combina computación, almacenamiento, conectividad de red y software de gestión en un solo dispositivo. Se puede elegir un propio servidor de hardware y configurar los discos a nuestro gusto, siempre y cuando el hardware sea compatible con el software del proveedor.

- **Servidor:** Un servidor es, en pocas palabras, una computadora, orientada al alojamiento y despacho de datos de distinto tipo. Los tipos de servidores más comunes son los que alojan webs: cada vez que se accede a un sitio web, en realidad se está estableciendo una conexión entre la computadora y un servidor, y lo que el navegador de Internet hace es pedirle a dicho servidor que le envíe el contenido del sitio web, de forma que pueda verse por pantalla.

2.2 APLICACIÓN

La infraestructura de servidores hiperconvergente comprende los elementos de hardware y software necesarios para sustituir el equipamiento de servidores actual basados en una tecnología horizontal tradicional de tres capas y realizar la gestión de los sistemas y el almacenamiento desde un punto único o centralizado. Esta solución incluye los recursos de procesamiento y almacenamiento necesarios para el correcto funcionamiento del

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

conjunto se nodos, así como las licencias de software y cualquier otro elemento necesario para interconexiones y su correcto funcionamiento. La finalidad es aportar simplicidad y flexibilidad; ya que los sistemas de almacenamiento integrados, los servidores y los conmutadores de red están diseñados para administrarse como un solo, facilitando de esta manera la migración de máquinas virtuales, así como mejora la automatización implicará un aumento en la eficiencia, eliminando los procesos manuales y la necesidad de contar con un equipo de operaciones con conocimientos aislados.

3. REQUISITOS

3.1 REQUISITOS GENERALES

NÚM.	DESCRIPCIÓN DE REQUERIMIENTOS
3.1	**INSTALACIÓN, CONFIGURACIÓN, MIGRACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA SOLUCIÓN DE SERVIDORES EN HIPERCONVERGENCIA Y SISTEMA DE COPIAS DE SEGURIDAD O BACKUP**
3.1.1	Instalación, Configuración y puesta en funcionamiento de la Infraestructura ON-PREMISES HIPERCONVERGENTE de 3 nodos que suministre (Servidores, procesamiento, almacenamiento y Redes, creación de Particiones Lógicas para plataformas de virtualización, Switches, SFPs para Switches, etc.) y de la solución de copias de seguridad junto con todos los elementos necesarios para la instalación y puesta en funcionamiento. La solución de servidores en hiperconvergencia y sistema de copias de seguridad deberá proveer un crecimiento modular y escalable, garantizando el aprovisionamiento tanto de cómputo, memoria y almacenamiento. Para ello se debe describir las características de escalamiento de la misma.
3.1.2	Efectuar un levantamiento de información (nombres, IP, sistemas operativos, capacidades en procesamiento/almacenamiento y RAM, servicios) y diseño, a la plataforma que suministre, para la **Migración de la totalidad de servidores virtualizados** (servidores virtuales que se encuentran en los servidores físicos). Así como una vez funcionales, generar de cada uno de ellos, las copias de seguridad en el sistema de copias de seguridad proporcionado. Así mismo, antes de iniciar la migración, se realizarán todas las copias de datos e imágenes de servidores ante una contingencia.
3.1.3	Entregar la suscripción del licenciamiento mínimo necesario por 3 años de la(s) plataforma(s) suministrada(s) (hipervisor y software de copias y recuperación), expedidos por el fabricante y registrado a nombre de la unidad, dirección, Nit y su respectivo key de activación. Garantizando la instalación de la última versión. Adicionalmente debe suscribirse un servicio de soporte profesional por parte del fabricante 24/7 de la solución ofertada tanto del hardware como del software de hiperconvergencia y sistema de copias o backup, para labores de soporte a la totalidad de las funcionalidades requeridas a instalar.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.1.4	En el diseño debe determinar y configurar la capacidad de memoria, disco y procesadores requerida en la Infraestructura que suministre de los servidores a virtualizar como: las bases de datos del Sistema de Información Académica y Folio de vida de cadetes Front y Back End en los diferentes ambientes de desarrollo y producción, servidor de Directorio Activo y DHCP, Servidor de cartelería Digital, Servidor ADconnet sincronización con el Office 365, Servidor consola de administración de redes LAN, Wifi y plataformas de Ciberseguridad, servidor de bases de datos de históricos, servidor códigos QR, Servidor Gestión Redes Algorius, entre otros.
3.1.5	Para efectos de la migración el contratista debe suscribir el licenciamiento Microsoft a nombre de la unidad, referente al software Datacenter y sistema Operativo necesario a suministrar; de acuerdo con los core, servidores físicos y virtuales que harán parte de la solución de Hiperconvergencia y sistema de copias de seguridad o backup, sobre ambientes Windows. Se deberá considerar la capacidad de cada nodo y garantizar una implementación adecuada, para cada una de las máquinas virtuales, sin incurrir en sub o sobre licenciamiento, garantizando la instalación de la última versión.
3.1.6	Se debe asegurar la integración y correcto funcionamiento entre las dos soluciones requeridas, sin afectar durante la implementación, los servicios informáticos de la red LAN y WAN de la unidad. Para ello, se deberán acordar tareas y ventanas de mantenimiento.

3.2 REQUISITOS ESPECÍFICOS

3.2.1	**INFRAESTRUCTURA DE SERVIDORES EN HIPERCONVERGENCIA** Describir las características tanto físicas como funcionales, para cada una de los requerimientos técnicos enunciados abajo, demostrado a través de fichas o catálogos emitidas por el fabricante de la solución, así:
3.2.1.1	**CARACTERÍSTICAS FÍSICAS**
3.2.1.1.1	El clúster deberá estar compuesta por mínimo tres (3) nodos
3.2.1.1.2	Cada nodo deberá incluir como mínimo uno (1) procesador de la familia Intel Xeon Gold o AMD EPYC con CPU 2.8 GHz o superior de al menos 16 Cores físicos.
3.2.1.1.3	Debe contar con memoria RAM de mínimo 1TB efectivas usables (total del clúster) en módulos DDR4 3200 MHz RDIMM o superior.
3.2.1.1.4	CONECTIVIDAD • Cada nodo deberá incluir como mínimo dos (2) puertos 10/25GbE SFP28 por nodo de hiperconvergencia o los necesarios para la interconexión de los nodos ofertados, con los conectores transceivers y fibras respectivas. • Se deben incluir los cables (poder, red, fibra óptica, entre otros), rieles de montaje y demás elementos requeridos para su instalación y puesta en funcionamiento.
3.2.1.1.5	La solución de hiperconvergencia debe soportar protocolos IPV4 e IPV6

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.1.6	Los nodos de hiperconvergencia ofertados no deben ser superiores a una (1) unidades de rack.
3.2.1.1.7	Cada nodo deberá contar con dos (2) fuentes de alimentación AC, Voltaje 230V/115V, frecuencia 50/60 Hz redundantes, para cada uno de los nodos de hiperconvergencia ofertados.
3.2.1.1.8	ALMACENAMIENTO INTERNO • La solución de hiperconvergencia debe garantizar como mínimo (27) TB efectivos usables, antes de compresión, de-duplicación o algoritmos de optimización, en almacenamiento con discos SSD o híbrido con discos SSD y HDD. • La solución de hiperconvergencia debe incluir compresión, sin licenciamiento adicional con las siguientes características: Debe estar integrada de forma nativa y debe ser global tanto para clúster con almacenamiento híbridos (SSD y HDD).
3.2.1.2	**CARACTERÍSTICAS FUNCIONALES DEL CLÚSTER**
3.2.1.2.1	La solución hiperconvergente debe basarse en softtware1 agnóstico y que pueda implementarse sobre múltiples fabricantes de hardware, procesadores como Intel o AMD, así como en nubes públicas. Esto con el fin de garantizar un esquema de nube híbrida de entrada, que permita centralizar las tareas de operación e integrar diferentes ambientes, brindando a la entidad múltiples opciones de despliegue y crecimiento.
3.2.1.2.2	La solución hiperconvergente debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y así mismo contar con un mecanismo nativo para automatizar la remediación de las desviaciones con respecto al hardening que puedan ocurrir durante todo el ciclo de vida de la solución, sin la ejecución de tareas manuales por parte de un administrador.
3.2.1.2.3	La solución hiperconvergente debe poder ejecutar de-duplicación y compresión completamente en software, sin requerir el uso de ningún hardware especializado para esta funcionalidad. Estas deben poder activarse o desactivarse por parte del administrador del sistema ya sea que ambas estén activas o solo una de las dos en el clúster.
3.2.1.2.4	Deberá traer instalado el hipervisor ofertado
3.2.1.2.5	Debe ser una solución con capacidad de crecimientos modulares en el mismo clúster, incrementado el número de servidores; que podrán ser de diferente familia y modelo del fabricante, con diferentes capacidades de procesamiento (diferente generación de procesadores), diferente tamaño de memoria y diferente tipo de almacenamiento (nodos con almacenamiento híbrido y nodos con almacenamiento solo de estado sólido), para suplir futuras ampliaciones y requerimientos de la entidad, garantizando siempre los niveles de desempeño de la solución sin degradar lo inicialmente adquirido.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.2.6	La solución hiperconvergente debe soportar exportar almacenamiento por bloques a servidores externos por medio de ISCSI.
3.2.1.2.7	La solución hiperconvergente debe presentar el contenedor de almacenamiento virtualizado al hipervisor de manera automática por medio de NFS, SMB v3.0 o iSCSI.
3.2.1.2.8	La solución hiperconvergente debe incluir funcionalidades para el manejo de las nuevas tendencias denominadas "contenedores", de tal forma que permita según la necesidad de la entidad optimizar el rendimiento y el empaquetamiento de aplicaciones en ambientes de Cloud.
3.2.1.2.9	La solución hiperconvergente debe soportar como mínimo Windows Guest Failover Clustering, funcionalidad que permite alta disponibilidad para las aplicaciones configuradas en clúster en una VM (Con sistema operativo Windows Server 2016 o Windows Server 2019 o Server 2022), para que transparentemente realice "failover" hacia otra VM ubicada en el mismo o en diferente host.
3.2.1.2.10	La solución hiperconvergente deberá entregar alto rendimiento al presentar los recursos de almacenamiento desde el mismo nodo en el cual se encuentra la máquina virtual, haciendo los requerimientos de IOPS para cada máquina virtual de forma local en el mismo nodo.
3.2.1.2.11	La solución hiperconvergente debe ser compatible para la virtualización de las plataformas (Windows Server 2016 o superior, Linux RedHat 8 o superior).
3.2.1.2.12	La solución hiperconvergente debe detectar de manera proactiva el daño de un disco, removerlo automáticamente del clúster y reconstruir de manera inmediata los datos que ahí se alojaban en los otros discos del clúster.
3.2.1.2.13	La solución hiperconvergente debe incluir la funcionalidad de replicación asincrónica que cumpla con los siguientes requerimientos básicos: - Replica a nivel de máquina virtual de forma granular. - Mecanismos de compresión y de-duplicación de los datos a ser replicados. - Replicación bidireccional entre dos centros de datos. - Posibilidad de limitar el ancho de banda usado por la replicación desde la interfaz de administración de la solución hiperconvergente. - Replicar máquinas virtuales entre dos hipervisores diferentes, convirtiendo la máquina virtual de un hipervisor a otro de forma automática.
3.2.1.2.14	La solución hiperconvergente debe soportar el respaldo y restauración de copias de las máquinas virtuales y archivos hacia la nube pública.
3.2.1.2.15	La solución hiperconvergente junto con el hipervisor, debe tener los drivers incluidos para la integración con Openstack, para mínimo los servicios de cómputo, imágenes, volúmenes y red.
3.2.1.2.16	El hipervisor ofrecido con la solución de hiperconvergencia, debe incluir la funcionalidad de ubicación inteligente de máquinas virtuales utilizando estadísticas de uso de CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	cargas de trabajo el mejor acceso posible a los recursos. Esta funcionalidad debe venir habilitada por defecto.
3.2.1.2.17	El hipervisor ofrecido con la solución de hiperconvergencia, debe permitir la definición de redes virtuales (SDN) mediante un switch virtual con soporte y mapeo de vLans, Link Aggregation, y visualización sobre los puertos físicos del switch TOR (Top Of Rack).
3.2.1.2.18	La solución hiperconvergente debe soportar al menos 3 diferentes tipos de vitualizadores tales como VMware ESXi, Microsoft Hyper-V Server y/o una distribución basada en KVM. Igualmente debe estar soportada la instalación del software en instancias de nube pública.
3.2.1.2.19	El hipervisor ofrecido con la solución de hiperconvergencia, debe proveer la capacidad de crear un camino directo de comunicación por cada vCPU hacia el almacenamiento sin implicar la instalación de ningún componente adicional.
3.2.1.2.20	El hipervisor ofrecido con la solución de hiperconvergencia, debe poder ser actualizado desde la misma consola gestión del sistema hiperconvergente a las últimas versiones sin disrupción del servicio.
3.2.1.3	**CARACTERÍSTICAS FUNCIONALES PARA LA ADMINISTRACIÓN Y MONITOREO DE LA SOLUCIÓN DE HIPERCONVERGENCIA**
3.2.1.3.1	La solución hiperconvergente deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de almacenamiento, firmware de los nodos e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales, ni solicitud de ventanas de mantenimiento ni indisponibilidad del servicio.
3.2.1.3.2	La solución hiperconvergente debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada como un servicio en cada uno de los nodos que componen la solución manteniendo una arquitectura de alta disponibilidad.
3.2.1.3.3	La solución de hiperconvergencia debe integrar herramientas de monitoreo y análisis predictivo de capacidad de cómputo, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad.
3.2.1.3.4	La interfaz de gestión debe estar construida sobre una interfaz HTML5 y ser administrado como mínimo a través de los navegadores Chrome, Firefox, Safari o Microsoft Edge.
3.2.1.3.5	La solución hiperconvergente deberá incluir con el hipervisor propuesto un portal de auto aprovisionamiento que permita la creación de proyectos, perfiles, usuarios, máquinas virtuales, plantillas de máquinas virtuales, de tal forma que la permita al cliente la automatización en la creación de servicios a usuario internos sin la necesidad de intervención de los administradores de infraestructura.
3.2.1.3.6	La interfaz deberá permitir gestión global y federada, es decir, desde un solo panel de administración se deberán gestionar todos los componentes de la solución hiperconvergente.
3.2.1.3.7	La interfaz para el auto aprovisionamiento debe soportar la integración con el directorio activo y certificados firmados por SSL, para el manejo de la autenticación de los usuarios que acceden.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.3.8	La interfaz para la administración debe permitir determinar en tiempo real el consumo de los recursos de CPU, Memoria RAM, y almacenamiento.
3.2.1.3.9	La interfaz de administración de solución de hiperconvergencia, deberá entregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias.
3.2.1.3.10	La interfaz para el auto aprovisionamiento debe contar con un catálogo donde se puedan configurar plantillas de máquinas virtuales y las imágenes que se deseen poner a disposición de los usuarios del portal.
3.2.1.3.11	La interfaz debe permitir la creación de diferentes roles de usuarios.
3.2.1.3.12	La interfaz de administración y monitoreo de la solución de hiperconvergencia deberá proveer accesos alternativos basados en SSH y/o interfaces seriales remotas, administración fuera de banda.
3.2.1.3.13	Soportar integración mediante el uso de REST API, a otras soluciones de administración para facilitar la integración con ambientes de monitoreo actuales.
3.2.1.3.14	La solución hiperconvergente deberá ser implementada por un especialista; por lo tanto, el proveedor de la solución durante la fase de presentación deberá certificar que está debidamente habilitado como distribuidor, al menos, en los 2 niveles superiores.
3.2.1.3.15	La interfaz debe permitir el análisis de ancho de banda utilizado por la misma, así como el ancho de banda de una máquina virtual.
3.2.1.3.16	La solución hiperconvergente debe distribuir los datos en el almacenamiento interno del clúster y adicionalmente replicarlos internamente para poder asegurar su disponibilidad, basados en Software y no en mecanismos legacy de hardware tipo RAID. Este factor de réplica debe poder ser configurado mediante dos o tres copias de los datos, dependiendo de las necesidades de la entidad.
3.2.1.3.17	La solución hiperconvergente debe incluir una funcionalidad que ejecute tareas de optimización automatizada de recursos, que permita realizar proyecciones de capacidad, tareas de planeación, basadas en tecnologías como machine learning.
3.2.1.3.18	La solución de hiperconvergencia debe incluir e integrar funcionalidades de aprovisionamiento, monitoreo y análisis predictivo de capacidad de cómputo, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad.
3.2.1.3.19	La solución hiperconvergente debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas.
3.2.1.3.20	La solución hiperconvergente debe incluir un catálogo de acciones que se inicien automáticamente, ante la activación de una alerta específica.
3.2.1.3.21	La solución hiperconvergente debe tener la capacidad de aprender el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales, en lugar de esperar a que las condiciones estén violando alguna regla, política o umbral. Todo esto basado en análisis de comportamiento / machine learning.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.3.22	La solución hiperconvergente debe incluir una función que permita crear areas automatizadas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración.
3.2.2	**SERVIDOR O SITEMA DE COPIAS O BACKUP** Entregar, instalar configurar y poner en funcionamiento un servidor para la realización de copias o backup y recuperación de datos de los entornos virtuales y físicos instalados en la solución hiperconvergente. Para ellos se deberán describir las características tanto físicas como funcionales, para cada una de los requerimientos técnicos enunciados abajo, demostrando estas a través de fichas o catálogos técnicos emitidas por el fabricante del sistema de copias, así:
3.2.2.1	Este servidor deberá ser proporcionado con la totalidad licenciamiento requerido (Sistema Operativo y Software de copias y recuperación del fabricante del sistema) por 3 años, a nombre de la entidad que garantice la correcta operación y funcionalidad de la solución de copias de seguridad ofertada. Además, debe contar con un servicio de soporte profesional por parte del fabricante 24/7 de la solución ofertada, para labores de soporte a las funcionalidades de backup y/o replicación.
3.2.2.2	**CARACTERÍSTICAS FÍSICAS DEL SERVIDOR O SISTEMA DE COPIAS O BACKUP**
3.2.2.2.1	El servidor o sistema de copias o Backup deberá incluir como mínimo dos (2) procesador de la familia Intel Xeon o equivalente AMD con CPU 2.7 GHz o superior de al menos 12 Cores físicos cada uno.
3.2.2.2.2	Memoria RAM de mínimo 64GB DDR5 4800MHz RDIMM o superior.
3.2.2.2.3	CONECTIVIDAD • El servidor deberá incluir como mínimo dos (2) puertos 10/25GbE SFP28 o los necesarios para la interconexión de los equipos ofertados, con los conectores transceivers y fibras respectivas. • Debe incluir los cables (poder, red, fibra óptica, entre otros), rieles de montaje y demás elementos requeridos para su instalación y puesta en funcionamiento.
3.2.2.2.4	Deberá contar con dos (2) fuentes de alimentación AC, Voltaje 230V/115V, frecuencia 50/60 Hz redundantes
3.2.2.2.5	El servidor o sistema de copias o Backup deberá contar como mínimo con 6 discos HDD de 8TB cada uno en RAID5.
3.2.2.3	**CARACTERÍSTICAS FUNCIONALES DEL SERVIDOR O SISTEMA DE COPIAS O BACKUP**
3.2.2.3.1	El sistema y/o solución de copias o backup deber proporcionar en una única consola capacidades de gestión para procesos de respaldo sin agentes para ambientes virtuales, replicación de máquinas virtuales on premises, gestión y distribución de agentes para

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	maquinas físicas y gestión de respaldos y recuperación de máquinas virtuales sobre ambientes cloud como Amazon AWS EC2 o Microsoft Azure.
3.2.2.3.2	El sistema y/o solución de copias o backup debe proporcionar una copia de seguridad eficiente "incremental para siempre" e incluir opciones de copias de seguridad completas y ad-hoc para cualquiera que sea la carga objetivo (VM Onpremises, VM Cloud Publica, NAS, Servidor Físico).
3.2.2.3.3	El sistema y/o solución de copias o backup debe admitir la copia de seguridad de VM directamente para ambientes hyperconvergentes sin licenciamiento adicional.
3.2.2.3.4	El sistema y/o solución de copias o backup debe detectar automáticamente las máquinas virtuales con el uso compartido de bus SCSI y excluirlas de la copia de seguridad.
3.2.2.3.5	El sistema y/o solución de copias o backup debe detectar automáticamente el espacio libre del datastore productivo y evitar la creación de snapshot para respaldo, si el espacio está por debajo del umbral definido.
3.2.2.3.6	El sistema y/o solución de copias o backup debe monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.
3.2.2.3.7	El sistema y/o solución de copias o backup deberá permitir tomar respaldos a partir de los Snapshots generados por el almacenamiento de producción de forma integrada, es decir, no deberá ejecutar tareas personalizadas o tareas adicionales por fuera de la consola de administración de respaldos.
3.2.2.3.8	El sistema y/o solución de copias o backup debe permitir la recuperación de Máquinas virtuales, archivos granulares de sistema operativo y de aplicación desde los snapshot's generados por el almacenamiento de producción
3.2.2.3.9	El sistema y/o solución de copias o backup no debe requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la ejecución de tareas de recuperación granular de aplicaciones.
3.2.2.3.10	El sistema y/o solución de copias o backup debe permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes en Máquinas Virtuales en ningún momento del proceso.
3.2.2.3.11	En los procesos de respaldo se debe permitir truncar los registros de transacciones o archivos de aplicaciones como Microsoft SQLServer, Microsoft Exchange y Oracle Database sin el uso de agentes en las máquinas virtuales en ningún momento del proceso.
3.2.2.3.12	El sistema y/o solución de copias o backup debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.
3.2.2.3.13	El sistema y/o solución de copias o backup debe permitir la copia de seguridad de los servidores de Windows configurados como un clúster de conmutación por error.
3.2.2.3.14	El sistema y/o solución de copias o backup debe proporcionar una portabilidad completa en cualquier archivo de respaldo ejecutado por la solución y no debe depender de ninguna

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	infraestructura de respaldo en un punto en el tiempo, por ejemplo, el catálogo central, para la recuperación.
3.2.2.3.15	El sistema y/o solución de copias o backup debe proporcionar tecnología de recuperación de respaldo de máquinas virtuales de forma instantánea (encendido en menos de 10 minutos y automática) desde el repositorio de respaldos ya sea que se encuentren On premises o sobre un almacenamiento de Objetos en una nube publica
3.2.2.3.16	El sistema y/o solución de copias o backup debe poder utilizar la copia de seguridad o réplica de la máquina virtual para iniciar la máquina virtual en un entorno de red aislado para fines de prueba o certificación de respaldos, sin necesidad de realizar una recuperación completa de la VM o procesos de pre-aprovisionamiento de almacenamiento
3.2.2.3.17	El sistema y/o solución de copias o backup debe poder escanear los datos de la máquina virtual a recuperar con un software antivirus antes de iniciar la restauración de la máquina al entorno de producción de forma integrada y automática. La solución debe abortar la operación de recuperación si se detecta malware.
3.2.2.3.18	El sistema y/o solución de copias o backup debe proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.
3.2.2.3.19	El sistema y/o solución de copias o backup debe facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente en el servidor destino
3.2.2.3.20	El sistema y/o solución de copias o backup debe permitir la recuperación de archivos de sistema operativo directamente sobre una máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.
3.2.2.3.21	El sistema y/o solución de copias o backup debe proporcionar una interfaz de usuario de autoservicio basada en la web con la capacidad de buscar un archivo específico en todas las copias de seguridad.
3.2.2.3.22	El sistema y/o solución de copias o backup no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.
3.2.2.3.23	El sistema y/o solución de copias o backup debe proporcionar una interfaz de usuario de autoservicio basada en web con la capacidad de examinar y recuperar elementos de Microsoft Exchange, bases de datos.
3.2.2.3.24	El sistema y/o solución de copias o backup debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.
3.2.2.3.25	El sistema y/o solución de copias o backup debe ser independiente del almacenamiento y debe contar con tecnología integrada de deduplicación y compresión.
3.2.2.3.26	El sistema y/o solución de copias o backup debe poder escalar tanto horizontal como verticalmente
3.2.2.3.27	El sistema y/o solución de copias o backup debe proporcionar un mecanismo fácil para expandir o adicionar el almacenamiento de respaldo de destino.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.3.28	El sistema y/o solución de copias o backup debe proveer la capacidad de implementar repositorio principal de respaldo de disco con características de Inmutabilidad, definiendo el número de días los cuales los archivos de respaldo no pueden ser modificados.
3.2.2.3.29	El sistema y/o solución de copias o backup debe admitir de forma nativa la copia de seguridad en cinta y no debe requerir software adicional.
3.2.2.3.30	El sistema y/o solución de copias o backup debe admitir medios de cinta y almacenamiento primario de disco tipo WORM.
3.2.2.3.31	El sistema y/o solución de copias o backup debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.
3.2.2.3.32	El sistema y/o solución de copias o backup debe proporcionar soporte para el almacenamiento de objetos Onpremises
3.2.2.3.33	El sistema y/o solución de copias o backup debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
3.2.2.3.34	El sistema y/o solución de copias o backup debe ofrecer inmutabilidad en el almacenamiento de objetos S3
3.2.2.3.35	El sistema y/o solución de copias o backup debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. incluso, ambas opciones se pueden habilitar en una misma política.
3.2.2.3.36	El sistema y/o solución de copias o backup debe encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.
3.2.2.3.37	El sistema y/o solución de copias o backup debe integrarse con SAML 2.0 para la autenticación extendida.
3.2.2.3.38	El sistema y/o solución de copias o backup debe proporcionar control de acceso basado en roles.
3.2.2.3.39	Deberá permitir la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma
3.2.2.3.40	El sistema y/o solución de copias o backup debe leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debe reconstruir automáticamente el bloque dañado con datos de producción.
3.2.2.3.41	El sistema y/o solución de copias o backup deberá poder programar tareas de encendido automático de las máquinas virtuales a partir de los respaldos y ejecutar tareas de verificación de sistema operativo y la disponibilidad de aplicaciones. Esta prueba no debe tener impacto en la red de producción. La solución debe proporcionar un informe de verificación de recuperación.
3.2.2.3.42	El sistema y/o solución de copias o backup debe escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.3.43	El sistema y/o solución de copias o backup debe presentar la tecnología de replicación directa de máquina virtuales.
3.2.2.3.44	El sistema y/o solución de copias o backup debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo
3.2.2.3.45	El sistema y/o solución de copias o backup debe alertar por adelantado si el repositorio de los respaldos se acerca a la capacidad.
3.2.2.3.46	Las copias secundarias de respaldo deberán ser independientes de la copia principal y podrán seleccionar diferentes puntos de retención con soporte a estrategias GFS
3.2.2.3.47	El sistema y/o solución de copias o backup debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de optimizar la utilización del ancho de banda.
3.2.2.3.48	El sistema y/o solución de copias o backup debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento con actualización dinámicamente la detección.
3.2.2.3.49	El sistema y/o solución de copias o backup debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.
3.2.2.3.50	El sistema y/o solución de copias o backup debe permitir el respaldo archivos a partir de los siguientes recursos: -CIFS -NFS -VSS Snapshot -SMB -Snapshot de dispositivos de almacenamiento Ontap Onpremises o Cloud
3.2.2.3.51	El sistema y/o solución de copias o backup debe permitir configurar en una única política la retención de corta duración en días o meses y movimiento de datos para retención de larga duración en meses y años para respaldo de datos no estructurados NAS
3.2.2.3.52	Las políticas de larga retención la solución podrá definir filtros de que tipo de datos respaldados desea mover a este nivel
3.2.2.3.53	El sistema y/o solución de copias o backup debe permitir la selección de cómo se debe gestionar el respaldo de los atributos de ACL, a nivel de carpeta o archivo y carpeta
3.2.2.3.54	El sistema y/o solución de copias o backup deberá poder seleccionar el nivel de compresión deseado por cada política de respaldo
3.2.2.3.55	El sistema y/o solución de copias o backup deberá permitir la encriptación de respaldo de NAS
3.2.2.3.56	El sistema y/o solución de copias o backup debe permitir la ejecución de tareas de revisión de salud de la cadena de respaldo de NAS para verificar la consistencia e integridad de forma programada o por demanda.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.3.57	El sistema y/o solución de copias o backup deber permitir la inclusión de scripts personalizados en las tareas de respaldo de NAS
3.2.2.3.60	El sistema y/o solución de copias o backup debe permitir los siguientes procesos de recuperación granular a partir de los respaldos de NAS: -Recuperación de archivos granulares y carpetas de CIFS y NFS -Recuperación de archivos granulares y carpetas de servidores gestionados de sistemas operativos Windows.
3.2.2.3.61	El sistema y/o solución de copias o backup deberá proveer la capacidad de devolver en un instante del tiempo toda una carpeta o recurso compartido completo sobre el recurso compartido original o uno totalmente diferente de locación incluso de almacenamiento a partir de los respaldos de NAS
3.2.2.3.62	El sistema y/o solución de copias o backup deberá permitir la recuperación completa de un recurso compartido de los puntos disponibles de respaldo de NAS
3.2.2.3.63	El sistema y/o solución de copias o backup deberá permitir la recuperación granular desde el repositorio de larga retención para los respaldos de NAS
3.2.2.3.64	El sistema y/o solución de copias o backup deberá incluir la capacidad de recuperación instantánea de un respaldo de NAS en forma de recurso compartido para ser accedido por la organización, este proceso no debe estar limitado por el tamaño del respaldo o los datos a acceder.
3.2.2.3.65	El sistema y/o solución de copias o backup debe proveer la capacidad de realizar réplicas de máquinas virtuales sin necesidad de generar snapshots y sin dependencia de hardware en origen y destino. La réplica de máquinas virtuales debe ser basada en política de RPO (máxima pérdida de datos permitida en caso de desastre) en intervalos de ejecución en segundos.
3.2.2.3.66	El sistema y/o solución de copias o backup debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas Onpremises y Cloud
3.2.2.3.67	El sistema y/o solución de copias o backup debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.
3.2.2.3.68	El sistema y/o solución de copias o backup debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.
3.2.2.3.70	El sistema y/o solución de copias o backup debe ofrecer la capacidad de generar alarmas y acciones de remedición en monitoreo de procesos y servicios de VM de ambientes Windows Onpremises
3.2.2.3.71	Debe proveer la capacidad de generar reportes personalizados basados en datos de inventario y uso de recursos de la plataforma virtual, como también de la plataforma de respaldo

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.3.72	El sistema y/o solución de copias o backup debe proporcionar informes de uso por cada uno de los almacenamientos usados por la solución, Onpremises o cloud
3.2.2.3.73	El sistema y/o solución de copias o backup debe proporcionar informes históricos y actuales de las sesiones de respaldo para todos los tipos de cargas configurados en la solución (Cloud - Onpremises)
3.2.2.3.74	El sistema y/o solución de copias o backup debe proporcionar informes tipo chargeback del uso de recursos
3.2.2.3.75	Deberá ofrecer un conjunto de reportes capaces de presentar la siguiente información: -Reportes que permitan la planificación de la capacidad. -Reportes que permitan la determinación de inefectividad en el uso de recursos. -Reportes que faciliten la visibilidad de tendencias negativas y anomalías de respaldo y uso de almacenamiento. -Envió automático y programado de reportes de auditoria para operaciones de recuperación y modificaciones a políticas de respaldos o replicación. -Tableros de control claros, presentables e integrables en sitios web.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

De acuerdo con las especificaciones, tanto los servidores nodos de hiperconvergencia como el servidor o sistema de copias o backups suministrados por el proveedor deben estar embalados en las cajas originales de fábrica y deben ser totalmente nuevos, sin uso previo. Esto garantiza que los equipos sean entregados en condiciones óptimas y cumplan con las expectativas de calidad y funcionamiento.

La instalación del software hipervisor, sistemas operativos y software de copias y replicación debe estar incluida en cada máquina y ser realizada antes de la entrega. Esto implica que los equipos entregados al Ejército Nacional deben contar con las licencias necesarias para su funcionamiento, y no se requerirá ningún licenciamiento adicional.

Cada equipo debe ser entregado con sus respectivos y manuales técnicos, manuales de operación, garantías, interfaces de conexión y software de configuración (drivers) en medios digitales originales. Estos componentes adicionales garantizan que se puedan utilizar y operar adecuadamente. Además, los manuales deben estar disponibles en idioma inglés y/o español, lo que facilitará el entendimiento y uso de los equipos por parte del personal del Ejército Nacional.

3.3.2 Rotulado.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

Los equipos suministrados por el proveedor deben contar con un sticker adhesivo que incluya la siguiente información:

1. Nombre de la empresa proveedora de los equipos.
2. Número del contrato correspondiente a la adquisición de los equipos.
3. Número telefónico de contacto para el soporte técnico.
4. Correo electrónico de contacto para el soporte técnico.

Este sticker adhesivo deberá colocarse en un lugar visible de cada equipo, de manera que sea fácilmente identificable y accesible. Esta información permitirá al personal contactar al proveedor en caso de requerir soporte técnico o asistencia relacionada con los equipos suministrados.

Es importante que el proveedor se asegure de que los stickers adhesivos estén claramente legibles y correctamente colocados en cada equipo, de modo que la información sea fácilmente visible y utilizable.

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1 Muestreo.

4.1.1 Muestreo. Sobre todos los compontes del sistema de la solución de hiperconvergencia y copias o backups a adquirir, se debe efectuar una inspección visual para verificar si cada componente cumple con los requisitos generales y requisitos de empaque y rotulado. Se debe tener presente que por sus características y complejidad serán inspeccionados la totalidad de los componentes que hacen parte del sistema integrado.

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. Cada uno de los componentes del sistema integrado, debe cumplir con lo establecido en la presente Especificación Técnica en los numerales 3.1 Requisitos Generales y 3.3 Requisitos de empaque y rotulado. Cuando no se cumpla el criterio de aceptación se rechazará el componente que no cumpla con los criterios establecidos.

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS.

4.2.1 Muestreo.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

Se requerirá la realización de pruebas de funcionalidad con el objetivo de garantizar que la configuración, integración e instalación de las soluciones sean apropiadas. En caso de que se identifiquen fallas técnicas en alguno de los componentes durante las pruebas, el proveedor deberá tomar las medidas necesarias para solucionarlas sin generar costos adicionales para el Ministerio de Defensa Nacional - Ejército Nacional.

Es responsabilidad del contratista garantizar que todas las soluciones implementadas funcionen correctamente y cumplan con los requisitos técnicos establecidos en el contrato.

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

Para verificar los requisitos específicos de la presente especificación se debe cumplir con el cien por ciento (100%) de lo establecido en el numeral 3.2 Requisitos Específicos mediante la verificación de su funcionamiento y mediante el método de inspección establecido en el numeral 5. Métodos de ensayo, de la totalidad de sus componentes. Cuando no se cumpla el criterio de aceptación se rechazará el componente que no cumpla con los criterios establecidos.

Es importante destacar que deben ser proporcionados por el proveedor sin generar costos adicionales para el Ministerio de Defensa Nacional - Ejército Nacional - Escuela militar de cadetes.

El proveedor es responsable de garantizar que los equipos y software funcionen correctamente y cumplan con las especificaciones técnicas establecidas en el contrato.

En caso de que alguno de los equipos presente una falla durante el período de garantía, es responsabilidad del fabricante proporcionar los materiales y/o piezas necesarias para su reparación o reemplazo.

- Estos materiales y/o piezas deben cumplir con las mismas características del equipo original o, en su defecto, ser de características superiores.

- El fabricante debe garantizar que los materiales y/o piezas utilizadas en la reparación o reemplazo sean compatibles y cumplan con los estándares y especificaciones técnicas requeridas. Esto asegura que el equipo vuelva a funcionar correctamente y se mantenga su rendimiento óptimo.

- Es importante que el proveedor y el fabricante especifiquen en el contrato y en los términos de garantía las condiciones y procedimientos para solicitar la reparación o reemplazo de un equipo defectuoso. Esto incluye los plazos de respuesta, los canales

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

de comunicación y cualquier requisito adicional que deba cumplirse para hacer efectiva la garantía.

De esta manera, el Ministerio de Defensa Nacional - Ejército Nacional - Escuela militar de cadetes puede contar con el respaldo necesario para garantizar el correcto funcionamiento de los equipos y su reparación o reemplazo en caso de presentarse alguna falla durante el período de garantía.

5. MÉTODOS DE ENSAYO

De acuerdo con la especificación, si durante las pruebas o instalación de las soluciones se detecta algún equipo defectuoso, es responsabilidad del proveedor reemplazar dicho equipo en un plazo máximo de 45 días calendario. El reemplazo debe ser realizado por un equipo nuevo, con las mismas características o superiores a las del equipo defectuoso.

El supervisor del contrato junto con el comité técnico evaluador realizará la verificación visual de los componentes de la solución de la siguiente manera:

- El proveedor realizará la entrega de los componentes en el respectivo almacén de comunicaciones.
- Se destapará las cajas de los componentes y se realiza la verificación del Datasheet y las Especificaciones Técnicas de acuerdo a la referencia de los equipos.
- Se realiza encendido y apagado de los equipos, para verificar el arranque y que encienda los equipos
- El proveedor realiza las respectivas configuraciones de los equipos y se llevarán para ser instalados.
- Se realiza la verificación de la administración y monitoreo de los equipos o sistemas; a través de la consola de administración.
- Se realiza la verificación del software de hiperconvergencia y servidor de copias de seguridad o backup.
- Se realizará visualización del certificado POE de la activación de las licencias, certificado emitido por el fabricante y se verificará en la consola de administración del mismo.

En caso de presentarse fallas en cualquiera de los elementos que componen de los sistemas o soluciones, se deberá brindar el soporte necesario, el cual debe incluir como mínimo:

- Cambio de equipos en caso de fallas: Si se identifica que un equipo específico está defectuoso, el contratista debe reemplazarlo por uno funcional sin costo adicional para el Ministerio de Defensa Nacional - Ejército Nacional – Unidad.
- Reemplazo de equipos por otros de iguales o superiores características: Si es necesario reemplazar un equipo, el contratista debe proporcionar uno con

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

características iguales o superiores para garantizar el correcto funcionamiento del sistema.

- Instalación de software: Si la falla está relacionada con el software, se debe realizar la instalación o reinstalación del software correspondiente para solucionar el problema.
- Configuraciones, puesta en producción y funcionamiento: El contratista debe llevar a cabo todas las configuraciones necesarias para poner en producción y asegurar el correcto funcionamiento del sistema después de cualquier reemplazo o reparación realizado.

Es importante destacar que el equipo de reemplazo no puede ser remanufacturado ni reparado, debe ser completamente nuevo. Esto garantiza que el equipo cumpla con los estándares de calidad y funcionalidad requeridos por el Ejército Nacional.

Además, el proveedor debe proporcionar los números de serie de los equipos de reemplazo para que se realicen los cambios pertinentes a nivel administrativo. Esto asegura un registro preciso de los equipos instalados y facilita la gestión de activos por parte del Ejército Nacional.

En resumen, el proveedor tiene la responsabilidad de reemplazar cualquier equipo defectuoso durante las pruebas o instalación con un equipo nuevo, sin remanufacturar ni reparar, dentro de un plazo máximo de 30 días. Los números de serie de los equipos de reemplazo deben ser proporcionados para fines administrativos.

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Ley 80 de 1993 “Por la cual se expide el Estatuto General de Contratación de la Administración Pública” y las demás normas que la modifiquen o aclaren.

- Ley 819 de 2003 "Por la cual se dictan normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal y se dictan otras disposiciones".

- Ley 1089 de 2006 "Por medio de la cual se regula la adquisición de bienes y servicios destinados a la defensa y seguridad nacional"

- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos"

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública"

- Decreto 1082 de 2015 ""Por medio del cual se expide el decreto único reglamentario del sector Administrativo de Planeación Nacional"

- Resolución 4213 de 2023 "Por la cual se modifica la Resolución 4130 de 2022 que expide el Manual de Contratación y de Convenios del Ministerio de Defensa Nacional"

- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos" y las demás normas que la modifiquen o aclaren.
- Ley 816 de 2003 "Por medio de la cual se apoya a la industria nacional a través de la contratación pública" y las demás normas que la modifiquen o aclaren.
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" y las demás normas que la modifiquen o aclaren.
- Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" y las demás normas que lo modifiquen o aclaren.
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Decreto 1082 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional" y las demás normas que lo modifiquen o aclaren.
- Decreto 103 del 20 de enero de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones" y las demás normas que lo modifiquen o aclaren.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Resolución de delegación 4519 del 27 de mayo de 2016 ""Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, a las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.

- Resolución No. 4130 del 16 de junio de 2022 "MANUAL DE CONTRATACIÓN Y DE CONVENIOS" del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.

- Resolución 2710 del 03 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" y las demás normas que la modifiquen o aclaren.

- Directiva de Seguridad de la Información del Ministerio de Defensa 2014-18 "Lineamiento de seguridad de la información para sector defensa" y las demás normas que la modifiquen o aclaren.

- Directiva permanente 00201 de 2017 "Lineamiento de ciberseguridad y Ciberdefensa para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.

- Directiva permanente 00221 de 2017 "Seguridad de la información para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.

6.2 ANTECEDENTES

Omitido

7. ANEXOS

Omitido

8. CONTROL DE REVISIONES:

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de especificación técnica **INFRAESTRUCTURA DE SERVIDORES EN HIPERCONVERGENCIA Y SERVIDOR DE COPIAS O BACKUPS No. JEMPP - CEDE6-DIPCO-ET-05692-COM-00**, con base a Solicitud Aval de la Especificación Técnica emitida ente CEDE6 No. 2024922006815763 de fecha 19 de marzo de 2024, Concepto Verificación catalogo compra Eficiente No. 2024922006772293 de fecha 196 de marzo de 2024, Estudio de Mercado No. 202492206773173	30/05/2024

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	de fecha 19 de marzo de 2024, estudio técnico de No. 2024922006813193 de fecha 19de marzo de 2024, Solicitud al BAICC No. 2024922011336063 de fecha 7 de mayo del 2024, Acta reunión mesa de trabajo No. 2024922005276786 de fecha 07 de mayo de 2024, Oficio de repuesta del BAICC No. 2024575011864853 de fecha 14 de mayo de 2024. Atendiendo el anexo E, de La Directiva de Planeamiento Logístico 00000050 20 de marzo del 2021 emitido Departamento Logístico. La Escuela Militar de Cadetes "General Jose María Córdova"-ESMIC, en la presente especificación técnica garantiza la pluralidad de oferentes. La Escuela Militar de Cadetes "General Jose María Córdova"-ESMIC, en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. La Escuela Militar de Cadetes "General Jose María Córdova"-ESMIC, técnica garantiza que la presente especificación fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional.	

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

COLOMBIA POTENCIA DE LA VIDA

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
EJÉRCITO NACIONAL
ESCUELA MILITAR DE CADETES

EJÉRCITO NACIONAL

ANEXO TÉCNICO

NÚM.	DESCRIPCIÓN DE REQUERIMIENTOS
1	**REQUERIMIENTOS TÉCNICOS DE LOS BIENES Y SERVICIOS, GARANTÍAS Y SERVICIOS CONEXOS**
1.1	En relación con la implementación; el contratista debe asumir todos los costos asociados con desplazamientos de su personal, transporte de equipos a los sitios, seguros locales, alquiler de instrumentos.
1.2	Si después de la instalación de los sistemas se llegase a presentar alguna falla en alguno de los elementos en mención a causa de los trabajos realizados, serán asumidos por el contratista quién debe repararlos sin costo alguno o hacer reposición por equipos o elementos de iguales o de mejores características.
1.3	El contratista garantizará que las actividades a realizar no afecten los servicios de red ni de otros equipos. Para ello se deberán establecer planes de contingencia.
1.4	La instalación de los nodos, la configuración del hipervisor y del sistema de copias de seguridad, se deberá realizar por parte del fabricante o en su defecto por el oferente, siempre y cuando este cuente con personal certificado en nivel profesional y/o de servicios de las soluciones ofertadas, para ello deberá anexar los correspondientes certificados de este personal junto con la oferta.
1.5	Se deberá entregar las claves de acceso de cada elemento activo de la(s) solución(es); así como los certificados del licenciamiento de software requerido a nombre de la Escuela Militar de Cadetes "General José María Córdova".
1.6	El proponente debe adjuntar certificación expedida por el fabricante (hiperconvergencia) no mayor a treinta (30) días de expedición a la fecha de cierre del presente proceso, donde se le acredite como distribuidor autorizado como mínimo en alguno de los 2 niveles más altos. Así mismo, adjuntar certificación de servicios y/o administración a nivel profesional o superior vigente de la solución de hiperconvergencia ofertada.
1.7	Certificación o aval de Fábrica en servicios de soporte: El proponente o uno de sus integrantes cuando éste sea un consorcio o unión temporal, debe presentar certificación del fabricante donde conste que está en la capacidad para proveer servicios de instalación "Socio de soporte autorizado" (ASP) para la infraestructura de hiperconvergencia.
1.8	El oferente deberá adjuntar junto con la oferta certificación(es) emitida(s) por la(s) casa(s) matriz/fabricante que lo acredite como distribuidor o implementador autorizado del sistema de copias de seguridad ofertado.
1.8	El proponente deberá aportar certificación de garantía mínima expedida por el fabricante de hiperconvergencia y del sistema de copias de seguridad no mayor a treinta (30) días de expedición a la fecha de cierre del presente proceso, la cual acredite que los bienes ofrecidos contarán como mínimo con TRES (3) años de garantía y soporte técnico suministrados directamente por el fabricante.
1.9	Todos los elementos activos y pasivos requeridos en la solución de hiperconvergencia y sistema o servidor de copias de seguridad, deben ser nuevos y originales. No se debe hacer reutilización de ningún material. Deberán ser entregados con sus respectivos manuales, cables de poder y accesorios.

1.10	Adjuntar en la oferta la ficha técnica de todos los elementos que integrarán tanto la solución de hiperconvergencia como sistema de backups (servidores, software o licencias y sistema de copias de seguridad); diligenciando en el cuadro/tabla de marca y referencias lo correspondiente. Así mismo, deberá incluir la URL y ficha técnica de la casa matriz o fabricante de cada elemento, donde se puedan validar cada una de las características requeridas, certificaciones y garantías exigidas.
2	**PERSONAL REQUERIDO**
2.1	EQUIPO DE TRABAJO El oferente debe disponer del personal necesario e idóneo para la instalación, configuración y/o puesta en funcionamiento de los equipos, elementos y/o software que integrarán la solución hiperconvergencia y el sistema o servidor de copias de seguridad. Para ello con la oferta debe anexar las hojas de vida de personal idóneo, copia de los correspondientes certificados de estudio, experiencia y fotocopia de la cédula para cada uno de los perfiles requeridos, en los cuales se certifique lo siguiente: **PERFIL 1: Un (1) GERENTE DE PROYECTO** **Rol**: Deberá encargarse de la gerencia de proyecto, documentación, organización y coordinación de actividades con la entidad. • Profesional en Ingeniería electrónica o telemática o de sistemas o telecomunicaciones o afines, entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional. • Postgrado con especialización o maestría en: Sistemas de Información o Gerencia de Proyectos o Telecomunicaciones o Gerencia de Proyectos de Ingeniería o Gestión de Proyectos de Ingeniería o Seguridad de la información o Gerencia de sistemas de información o Gerencia de Proyectos de Telecomunicaciones o Gerencia de proyectos con certificación PMP vigente, expedida por el Project Management Institute PMI. **PERFIL 2: DOS (2) EXPERTOS TÉCNICOS** **Rol**: - Gestionar y articular técnicamente tanto de forma interna como externa, los componentes técnicos de las soluciones ofertadas. Deberá apoyar la revisión de las soluciones, factores de calidad de las implementaciones y supervisión a los procesos en implementación hasta su entrega. - Ejecución de actividades técnicas para implementación de la(s) solución(es) de hiperconvergencia • Los dos perfiles deberán ser Profesional en Ingeniería electrónica o telemática o de sistemas o telecomunicaciones o afines, entendidas como aquellas que

	comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional. • Con especialización o maestría en: Sistemas de Información o Gerencia de Proyectos; Gerencia de proyectos Informáticos o Telecomunicaciones o Gerencia de Proyectos de Ingeniería o Gestión de Proyectos de Ingeniería o Gerencia de sistemas de información o Gerencia de Proyectos de Telecomunicaciones o gerencia de proyectos de ingeniería o afines. • Experiencia certificada, como mínimo debe haber participado en 4 proyectos de implementación de la solución de Hiperconvergencia. Adjuntar certificaciones firmadas por las entidades donde se llevó a cabo la implementación. • Los dos perfiles deberán contar con certificación técnica vigente del fabricante de Hiperconvergencia ofertado, en nivel Profesional y uno de ellos deberá aportar certificado técnico vigente del fabricante de la solución de copias de seguridad. Nota: - El supervisor evaluará el desempeño laboral del personal asignado, quien estará en facultad de solicitar su reemplazo si lo considera necesario, en dado caso el contratista deberá reemplazarlo en un tiempo no mayor a cinco (5) días hábiles luego de la solicitud formal por parte del supervisor del contrato. - El contratista debe garantizar que los daños que cause a cualquier elemento o sistema existente en la Escuela Militar de Cadetes serán asumidos por el adjudicatario quién debe repararlos sin costo alguno o hacer reposición por equipos o elementos de iguales o mejores características.
2.2	- El contratista después de perfeccionado el contrato, en un plazo máximo de cinco (5) días hábiles, enviará toda la documentación requerida por el EJC para elaborar los estudios de seguridad del personal propuesto para la implementación de las redes, previas coordinaciones con el supervisor del contrato - El contratista garantiza la continuidad y permanencia, en tiempo completo, del personal asignado inicialmente al proyecto para la implementación de la solución. Cualquier cambio de personal del contratista será aprobado por el supervisor designado por la ESMIC, previa solicitud escrita presentada con anticipación, ocho (08) días calendario. - Si no existe entera satisfacción de la ESMIC, acerca de los profesionales asignados para implementar las redes objeto de este proceso, previa notificación por escrito al contratista, este asignará un nuevo profesional o profesionales en un tiempo máximo de cinco (05) días calendario contados a partir de la fecha de la notificación. - El contratista cumplirá todas las normas de SEGURIDAD INDUSTRIAL en el desarrollo del contrato y garantizar los cuidados y precauciones necesarias para el desarrollo del

	mismo. Igualmente garantizará que los sitios de trabajo queden ordenados y aseados luego de efectuada sus labores. - Se aclara que entre el personal empleado por parte del contratista para desarrollar el objeto del contrato y la ESMIC, no existirá vínculo laboral alguno. - El contratista entregará junto con la oferta las copias de las certificaciones expedidas por los fabricantes en la cual conste que el personal que participará en la ejecución del contrato, debe ser idóneo en instalación del cableado estructurado, instalación y puesta de la(s) solución(es). - El contratista deberá entregar al supervisor del contrato, la documentación necesaria para la instalación. - El personal asignado a cada proyecto debe tener su respectivo carnet que lo identifique como miembro activo de empresa contratista, así mismo deberá tener chaleco o uniforme con el logo o nombre de empresa, que lo identifiquen plenamente.
3	VISITA TÉCNICA Y PLAN O CRONOGRAMA DE TRABAJO El contratista realizará una visita en sitio para verificar la infraestructura tecnológica, configuraciones de la escuela para la implementación de las soluciones. Dentro de los subsiguientes cinco (05) días calendario deberá entregar al supervisor el diseño y/o arquitectura de la implementación propuesta, junto con el cronograma de actividades indicado en este, las ventanas de mantenimiento y los planes y/o procedimientos de contingencia a que haya lugar, la cual será aprobada por el Jefe de la Sección B6.
4	GARANTÍA TÉCNICA DE LOS ELEMENTOS DE LAS SOLUCIONES - El contratista entregará al supervisor, certificado de suscripción de garantías técnica; así como un servicio de soporte técnico por el fabricante de la solución de hiperconvergencia y del sistema o servidor de copias de seguridad, sin costo adicional para la ESMIC, por tres (3) años. - A partir de la finalización del contrato con la firma de recibido a satisfacción entre el supervisor del contrato y el representante legal de la empresa contratista, iniciará la vigencia de la garantía técnica del servicio de soporte prestado, en donde se obliga a realizar la aplicación de las actualizaciones y/o ajustes de los componentes físicos y lógicos intervenidos, garantizando la correcta integración, funcionamiento y demás bienes entregados. - Una vez efectuada la entrega se deberá proporcionar los documentos que considere para ilustrar y dar a conocer claramente la metodología y/o pasos que deberá seguir la escuela para solicitar y ejecutar el servicio de garantía y soporte por parte del fabricante.

	- El contratista debe garantizar el cambio de hardware y software de la solución de hiperconvergencia y sistema de copias de seguridad, por una nueva, de iguales o superiores características técnicas, cuando se presenten fallas técnicas, durante el tiempo de garantía, sin ningún tipo de costo para la entidad. Entendiéndose como falla, el no funcionamiento de cualquiera de los componentes de hardware y software de la solución de hiperconvergencia, de acuerdo con los Acuerdos de Niveles de Servicio ANS acordados entre el contratista y el supervisor. - El contratista durante el tiempo de garantía (3 años), realizará la entrega de nuevas actualizaciones, sin costo de las licencias y/o firmware (Nuevas versiones, actualizaciones, mejoras e instalación de nuevas funcionalidades y mantenimiento de la licencia de la presente especificación técnica) y a través de los servicios de soporte con el contratista se apoyará a la Sección B6 en la instalación de las mismas. Con anterioridad, deberá liberar las actualizaciones probadas y las liberadas, indicando a la escuela las actividades de aseguramiento a realizar.
5	DOCUMENTACIÓN <u>INFORMES</u> - Informes semanales y/o mensuales del avance y actividades realizadas; de acuerdo al plan y cronograma de trabajo acordado durante la ejecución del contrato. - Planes de operación, contingencia y ventanas de mantenimiento. - Informe de Pruebas técnicas de operación y mantenimiento. <u>DOCUMENTACIÓN FINAL</u> Previo al acta de recibo a satisfacción del contrato, el contratista entregará al supervisor del contrato, un documento original impreso en una carpeta tipo folder y copia en medio magnético con toda la información (CD). El archivo debe incluir como mínimo: - Diagramas de conectividad y de la arquitectura implementada. - Hoja de vida Digital de los nodos físicos y servidores virtuales creados de las dos soluciones. Así como el inventario de equipos y actualización del sistema Algorius. - Configuraciones de software, copias e imágenes de seguridad de los servidores y bases de datos. - Certificaciones de las suscripciones de licenciamiento y procedimiento, usuarios y contraseñas para generación de soportes de mesa de ayuda. - Fotografías del antes, durante y después. - Manuales técnicos - Documentos de garantías y soportes técnicos del(os) fabricantes y contratista de los equipos y software.

ESMIC

	- Contraseñas de administración, en una aplicación de manejo de contraseñas segura, que deberá ser instalada en la Sección B6 de la ESMIC. Con la oferta se deberá establecer marca y referencia de la aplicación a entregar.
6	TRANSFERENCIA TECNOLÓGICA El contratista deberá realizar transferencia de conocimiento durante el proceso de la instalación, configuración y puesta en marcha de la solución de Hiperconvergencia y sistema de coipas de seguridad, así como capacitación durante mínimo 20 horas para hasta 5 funcionarios designados por la supervisión, en la administración de la totalidad de herramientas que integran la solución de hiperconvergencia y sistema de copias de seguridad. Esta deberá ser construida y presentada por el contratista, conteniendo los temas necesarios para la apropiación técnica del proyecto y deberá ser aprobada por el supervisor.
7	SERVICIO DE SOPORTE TÉCNICO DEL FABRICANTE Y CONTRATISTA SOPORTE FABRICANTE Con la oferta se debe adjuntar documento firmado por el oferente tanto de la solución de hiperconvergencia y del sistema de copia de seguridad, del tipo y alcance de servicio y de soporte a adquirir con el(os) fabricante(s) por tres (3) años. Deberá ser mínimo bajo las siguientes condiciones: - El contratista suscribirá y entregará durante la ejecución, el certificado para la Escuela Militar de Cadetes de un servicio de soporte Profesional o del más alto nivel con el fabricante durante 3 años, tanto para la solución de hiperconvergencia como del servidor de copias de seguridad, con atención 7x24x365, envío e instalación de la totalidad de los equipos o componentes de software y de partes nuevas de fábrica. - El soporte técnico de primer nivel o alta criticidad de las soluciones requeridas debe ser prestada directamente por el fabricante durante 3 años. SOPORTE OFERENTE Y/O CONTRATISTA Durante la vigencia de la garantía técnica, el oferente debe presentar con la oferta la descripción del servicio de soporte técnico de nivel 1 y 2 a realizar, prestado directamente por su personal, mediante una mesa de ayuda propia con software de certificado ITIL, el cual debe anexar adicionalmente en la propuesta. Este servicio debe contar con las siguientes características mínimas: - Acceso ilimitado de soporte a través de atención telefónica y/o correo electrónico, y acceso remoto; a través de un usuario con contraseña de la ESMIC. - El horario de soporte técnico debe ser 24x7x365 con 4 horas de respuesta.

	- En caso de no dar solución a la falla por estos medios deberá el comitente vendedor asignar un ingeniero especializado para acudir al sitio, con un tiempo de respuesta máximo de cuatro (4) horas.
	- Corregir las fallas en el servicio o en los bienes suministrados que resulten defectuosos dentro del plazo que le señale el supervisor. En caso de que sean fallos recurrentes sobre los equipos entregados, estos deberán serán remplazados en su totalidad por parte del contratista, con un plazo máximo de 30 días calendario.
	- Entre las actividades de mantenimiento se debe contemplar:
	  - Creación de tickets vía telefónica o correo electrónico.
	  - Soporte técnico de la solución en compañía del fabricante.
	  - Actualizaciones de software por la vigencia de la renovación, a versiones mayores (upgrades) y mejoras menores (updates).
	  - La línea de contacto debe permitir la apertura de tickets tanto de soporte y garantía y el reporte de las posibles fallas que presenten, actualizaciones, entre otras.
	  - En caso que se reporten fallas por parte de la ESMIC, el contratista debe llevar a cabo las siguientes actividades mínimas:
	  - Diagnóstico inicial por medio de una conexión remota a los equipos.
	  - Realizar todo el protocolo de pruebas necesario para validar cuál es el origen de la falla reportada y en lo posible dar solución remota.
	  - Brindar soporte en sitio, con la finalidad de garantizar la adecuada operación de las soluciones instaladas.
	
	Durante la ejecución, el contratista deberá entregar dentro la documentación del proyecto tanto la documentación de certificados de garantías técnicas del fabricante para cada una de las soluciones como las suscripciones de los servicios de soporte técnico de este. Así como entregar el procedimiento y los ANS, contactos, usuarios y contraseñas de la mesa de ayuda requerida.

8	CONFIDENCIALIDAD DE LA INFORMACIÓN El contratista y los recursos humanos que formarán parte del equipo de trabajo deberán firmar al inicio del contrato un acuerdo de confidencialidad donde garantizan la confidencialidad de la información Institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional así mismo a dar cumplimiento a: - Ley 1581 de 2012 de Protección de datos personales - Ley 1712 de 2014 Acceso a la información pública - Ley 1273 de 2009 Modificación del Código Penal -bien jurídico tutelado "protección

	- de la información y de los datos". - Ley 23 de 1982 de Derechos Autor y Ley 1915 de 2018. El contratista deberá aceptar y permitir que la Escuela Militar de Cadetes "General José María Córdova", efectúe los estudios de seguridad al personal que considere necesario, para garantizar la seguridad de su infraestructura computacional e información. En tal virtud, adoptará todas las medidas necesarias para impedir la duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida de información. Bajo ninguna circunstancia dicha información y/o documentación podrá ser utilizada por el contratista para fines distintos al desarrollo del contrato respectivo. Al finalizar la ejecución del contrato toda la información y documentos entregados La Escuela Militar de Cadetes, deberán ser retornados

Elaboró	Revisó	Aprobó
TO JUAN CARLOS SUÁREZ Ingeniero TIC-B6 ESMIC	ST. CASTIBLANCO ROSERO Oficial TIC-B6 ESMIC	CR. GEOVANNY ANDRÉS CORTÉS MOLINA Subdirector ESMIC

ESMIC