MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
EJÉRCITO NACIONAL
PATRIA HONOR LEALTAD DIVISIÓN DE AVIACIÓN ASALTO AEREO

Al contestar, cite este número
Radicado No. 2026519030438923: MDN-COGFM-COEJC-SECEJ-JEMOP-DAVAA-D6

Bogotá, D.C., 21 septiembre de 2026

Señor Teniente Coronel
GUSTAVO ADOLFO CAÑON ROMERO
Director Central Administrativa y Contable Especializada Telemática.
Facatativá- Cundinamarca

Asunto: ANEXO No. 01 – ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

Con toda atención me permito enviar al señor Teniente Coronel Director de la Central Administrativa y Contable Especializada de Telemática, los soportes para iniciar el estudio previo del plan de necesidades del proceso cuyo objeto es "SUMINISTRO, ADQUISICION, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE SISTEMA DE RED DE DATOS PARA LAS UNDIADES DEL EJERCITO, (INCLUYE: SUMINISTRO DE LOS BIENES, CARGUE, DESCARGUE, TRANSPORTE, MANO DE OBRA, ELEMENTOS Y ACCESORIOS NECESARIOS PARA SU INSTALACIÓN, USO DE HERRAMIENTAS MENORES Y EQUIPOS DE PROPIEDAD DEL PROVEEDOR QUE SEAN NECESARIAS PARA LA INSTALACIÓN, CONFIGURACIÓN, PRUEBAS, Y PUESTA EN FUNCIONAMIENTO DE LA SOLUCIÓN OFERTADA) A TODO COSTO Y TODO INCLUIDO, DE ACUERDO CON LAS ESPECIFICACIONES TÉCNICAS DEL ANEXO", como se menciona a continuación:

RELACIÓN BIENES Y SERVICIOS A ADQUIRIR.

ADQUISICION Y PUESTA EN FUNCIONAMIENTO DE EQUIPOS DE BACKUP MULTIPROPOSITO, EQUIPO ACTIVO SWITCH CORE Y ACTIVIDADES DE MANTENIMIENTO PREVENTIVO, CORRECTIVO E INSTALACIÓN DE PUNTOS DE DATOS Y ELECTRICOS								
ÍTEM	CÓDIGO DANE	DESCRIPCIÓN DEL BIEN Y/O SERVICIO	UNIDAD MEDIDA	EXISTENCIAS (STOCK - INVENTARIOS)	NECESIDAD	UNSPSC (CCE)	CÓDIGO MATERIAL SAP (OPCIONAL)	CÓDIGO OTAN - NOC (OPCIONAL)
1		SOLUCIÓN DE INFRAESTRUCTURA DE RESPALDO, diseñada para la protección, resguardo y recuperación de la información institucional, de conformidad con los requisitos establecidos en el documento No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00. Se consideran incluidos los apartados	UNIDAD	0	1			

		técnicos referenciados en el anexo correspondiente: 3.2.1.1.1, 3.2.1.1.4, 3.2.1.1.5, 3.2.1.1.7, 3.2.2.2.1 al 3.2.2.2.71, así como los numerales del documento base especificados en el anexo: 3.2.2.1.1, 3.2.2.1.2, 3.2.2.1.3, 3.2.2.1.5, 3.2.2.1.6, 3.2.2.1.9, 3.2.2.1.10, 3.2.2.1.11, 3.2.2.1.12, 3.2.2.1.14, 3.2.2.1.15, 3.2.2.1.16, 3.2.2.1.17, 3.2.2.1.18 y 3.2.2.1.19.						
2		INTERRUPTOR DE TRANSFERENCIA DE RACK HÍBRIDO INTELIGENTE. Para el soporte para la solución de infraestructura de BACKUP, orientado a garantizar la continuidad operativa y la disponibilidad de los equipos de la solución. De acuerdo con requerimientos establecidos en el documento No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00, incluyendo los numerales técnicos indicados en el anexo correspondiente: 2.2.3.1 hasta 2.2.3.27.	UNIDAD	0	1			
3		SWITCH CORE 24 PUERTOS 10Gb SFP+ con uplinks 40/100Gb, arquitectura modular, fuentes redundantes, instalación, configuración, integración, licenciamiento avanzado y soporte 24x7 por 3 años. De acuerdo con requerimientos establecidos en el documento No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, que incluye los numerales técnicos especificados en el anexo correspondiente: 3.3.1.2 al 3.3.1.45, abarca todos los aspectos establecidos en dicha documentación para su adecuada interpretación y cumplimiento.	UNIDAD	0	1			
4		SERVICIO DE MANTENIMIENTO PREVENTIVO A PUNTO DE DATOS Existentes, incluye inspección, normalización, certificación y pruebas de desempeño.	UNIDAD	0	141			
5		SUMINISTRO DE INSTALACIÓN DE PUNTO DE DATOS CATEGORÍA 6A certificado, con canalización, accesorios, rotulado y pruebas bajo norma TIA/EIA. De acuerdo con requerimientos establecidos en el documento No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 incluyendo los numerales técnicos referidos en el mismo anexo: 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10 y 4.11	UNIDAD	0	25			
6		SUMINISTRO DE INSTALACIÓN DE PUNTO ELÉCTRICO DOBLE TIPO NORMA Y REGULADO, con canalización, conexión y pruebas de funcionamiento.	UNIDAD	0	25			

7		SERVICIO DE MANTENIMIENTO PREVENTIVO A RACK DE COMUNICACIONES, incluye limpieza técnica, organización de cableado y normalización de patch panels.	UNIDAD	0	2			
8		SERVICIO DE MANTENIMIENTO PREVENTIVO A SWITCHES DE RED, incluye limpieza, verificación de conexiones y pruebas básicas de funcionamiento.	UNIDAD	0	13			

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE FORTALECIMIENTO, MANTENIMIENTO Y MODERNIZACIÓN DE LA INFRAESTRUCTURA CRÍTICA DE CONECTIVIDAD Y RESPALDO TECNOLÓGICO	
NÚM.	**DESCRIPCIÓN DE REQUERIMIENTOS**
1.	**INFRAESTRUCTURA DE BACKUP**
1.1	Solución de infraestructura de backup, orientada a la protección, respaldo y recuperación de la información institucional De acuerdo con requerimientos establecidos en el documento No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00
1.2	El proponente deberá tener en cuenta únicamente los numerales relacionados en el presente anexo de especificaciones técnicas adicionales.
1.3	Características de la Infraestructura de Almacenamiento, conforme a los numerales **3.2.1.1.1** y del **3.2.1.1.4, 3.2.1.1.5, 3.2.1.1.7** relacionados con la conformación del clúster, características de procesamiento, memoria, conectividad, protocolos soportados y demás condiciones generales de la plataforma. Aclarando lo siguiente: • Procesador: Cada nodo ofertado deberá incluir mínimo 1 procesadores de al menos 8 Cores físicos cada uno, mínimo procesador Intel Xeon 2.0GHz • Memoria RAM: La solución completa debe contar con memoria RAM de mínimo 384 GB RAM DDR5 5600MHz o superior • La solución de almacenamiento debe tener las capacidades de gestión para mínimo 35 TiB
1.4	El almacenamiento distribuido debe ser garantizado después de la caída de uno de los nodos de acuerdo al requerimiento técnico y lo establecido en el presente anexo adicional. Se deberá contemplar la capacidad de almacenamiento con las funcionalidades para mínimo 35 TiB.
1.5	La solución de almacenamiento debe incluir compresión, con las siguientes características: • Debe estar integrada de forma nativa.
1.6	Características de la solución de BACKUP, **conforme a los numerales 3.2.2.2.1 al 3.2.2.2.71**, los cuales establecen las capacidades y funcionalidades requeridas para la ejecución de los procesos de respaldo, recuperación y restauración de información.
1.7	Adicionalmente a las especificaciones técnicas de este anexo, la solución de infraestructura de backup deberá cumplir, como mínimo, con los requerimientos técnicos del documento No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00, los cuales hacen parte integral e indivisible del alcance técnico, de conformidad con los numerales **3.2.2.1.1, 3.2.2.1.2, 3.2.2.1.3, 3.2.2.1.5, 3.2.2.1.6, 3.2.2.1.9, 1.10, 3.2.2.1.11, 3.2.2.1.12, 3.2.2.1.14, 3.2.2.1.15, 3.2.2.1.16, 3.2.2.1.17, 3.2.2.1.18 y 3.2.2.1.19.**
1.8	La solución deberá ofrecer almacenamiento de objetos nativo con acceso S3 (REST API) para aplicaciones y servicios, soportando respaldo, retención de largo plazo, Big Data y DevOps. Esta capacidad debe estar integrada y administrada desde una consola unificada, sin componentes externos, garantizando simplicidad

	operativa, seguridad avanzada y escalabilidad continua.
1.9	El servicio de almacenamiento de objetos deberá incorporar WORM nativo, garantizando la inmutabilidad de los datos durante el período definido, sin modificación ni eliminación, incluso por usuarios administrativos, asegurando cumplimiento normativo e integridad de la información crítica
1.10	La plataforma de almacenamiento de objetos deberá soportar de forma nativa Object Lock, garantizando la inmutabilidad de los datos y su recuperación íntegra, sin componentes adicionales, asegurando cumplimiento de políticas de retención y protección de la información crítica en entornos regulados.
1.11	La solución deberá soportar de forma nativa el versionado de objetos S3, permitiendo conservar y recuperar versiones sin componentes externos ni requerimientos adicional, garantizando trazabilidad, protección de datos y continuidad operativa en entornos críticos..
1.12	La solución deberá permitir escalabilidad horizontal mediante la adición de nodos, sin cabinas externas ni gateways, garantizando crecimiento lineal sin interrupciones y simplicidad operativa. Asimismo, debe integrarse de forma nativa con Active Directory y/o LDAP, ofreciendo control de accesos basado en roles y políticas centralizadas para asegurar cumplimiento normativo y protección de datos en entornos críticos..
1.13	La solución de consolidación de almacenamiento para S3 deberá soportar de forma nativa COSI (Container Object Storage Interface), permitiendo a aplicaciones Kubernetes autoaprovisionar almacenamiento sin intervención manual, garantizando automatización, simplicidad operativa, compatibilidad con entornos de contenedores y escalabilidad en arquitecturas híbridas y multicloud.
1.14	La solución deberá ofrecer de forma nativa la consolidación de múltiples servicios de almacenamiento en una única plataforma, soportando simultáneamente protocolos de archivos (NFS y SMB) y almacenamiento de objetos mediante protocolo S3, sin depender de appliances externos. Esta integración debe ser inherente a la arquitectura de la solución, garantizando rendimiento consistente, alta disponibilidad y administración unificada para todos los servicios, evitando complejidad operativa y puntos únicos de falla.
1.15	La solución deberá ofrecer la capacidad nativa de exportar almacenamiento para la construcción de servidores de archivos mediante protocolos SMB (Server Message Block) y NFS (Network File System), de forma simultánea y sin requerir gateways externos ni componentes adicionales. Esta funcionalidad debe estar integrada en la misma plataforma, garantizando alto rendimiento, administración unificada y compatibilidad con entornos corporativos, reduciendo complejidad operativa y puntos únicos de falla.
1.16	La solución deberá incluir de forma nativa analítica avanzada para servidores de archivos SMB y NFS, administrada desde una consola unificada y sin herramientas externas, permitiendo analizar consumo y tendencias de capacidad, antigüedad de datos, distribución por tamaño y tipo, actividad de usuarios y archivos, eventos de acceso no autorizado, alertas por anomalías, auditoría detallada, detección y mitigación de ransomware en tiempo real y generación de reportes personalizados. Estas capacidades deben garantizar trazabilidad, seguridad avanzada y cumplimiento normativo, sin aumentar la complejidad operativa ni costos adicionales.
1.17	La solución deberá soportar de forma nativa políticas de cuota por usuario o recurso compartido, con alertas automáticas al aproximarse a los límites definidos, permitiendo acciones preventivas y asegurando cumplimiento de políticas corporativas sin herramientas externas ni requerimientos adicionales.
1.18	El oferente deberá presentar, como documento independiente de la oferta, un certificado emitido por el fabricante que certifique su condición de canal autorizado, así como la autorización para distribuir y brindar soporte a los productos adquiridos.
1.19	Seguridad de firmware. Los nodos que conformen la infraestructura de almacenamiento y respaldo deberán incorporar, como mínimo, las siguientes capacidades: • Contar con una raíz de confianza basada en silicio o mecanismo de hardware inmutable que permita validar criptográficamente la integridad del firmware del subsistema de administración y de los componentes críticos durante el proceso de arranque. • Disponer de un repositorio local o embebido para firmware y controladores que permita almacenar conjuntos de actualización y recuperación, así como ejecutar reversión o recuperación ante firmware comprometido

	hacia una versión previamente validada o un estado seguro de fábrica. • Contar con un subsistema dedicado e independiente para la protección de secretos y claves criptográficas, resistente a manipulación física y con soporte para requisitos de protección de hardware FIPS 140-3 Nivel 3. • Permitir la ejecución programada de verificaciones de integridad del firmware y la configuración de acciones de recuperación cuando se detecten fallas de validación o compromiso de componentes críticos. • Disponer de un panel de seguridad que permita visualizar el estado de los controles relevantes, identificar riesgos de configuración y consultar el detalle y las recomendaciones de remediación correspondientes. • Permitir recuperación segura de firmware crítico a un estado conocido como seguro y capacidad de reversión de firmware cuando se requiera.
1.20	Administración remota embebida. Cada nodo deberá incorporar un subsistema de administración remota fuera de banda, independiente del sistema operativo, que cumpla como mínimo con las siguientes capacidades: • Consola gráfica remota basada en navegador, control virtual de encendido, apagado y reinicio, y medios virtuales para arranque remoto mediante imágenes o dispositivos USB/CD/DVD soportados. • Actualización remota de firmware y componentes de software mediante archivos, imágenes o repositorios de actualización, sin requerir presencia física frente al servidor. • Puerto físico dedicado para administración remota con velocidad mínima de 1 Gb/s. • Administración sin agentes a través del puerto de gestión fuera de banda y monitoreo de la salud del sistema sin dependencia de agentes instalados en el sistema operativo. • Monitoreo y registro de cambios en el hardware, configuración del sistema y eventos relevantes, con información utilizable para diagnóstico y resolución de fallas. • Autenticación multifactor, cuentas de usuario locales o integradas con servicios de directorio y control de acceso basado en roles y privilegios. • Capacidad de consola remota multiusuario conforme al licenciamiento ofertado y función de grabación/reproducción de la consola para revisar secuencias de arranque o eventos de falla. • Protección de las comunicaciones de administración mediante HTTPS/TLS y cifrado basado en AES. • API RESTful compatible con Redfish para inventario, configuración, monitoreo y automatización de tareas de administración. • Monitoreo histórico del consumo de energía y soporte de funciones de limitación de potencia cuando sean soportadas por la configuración del servidor.
1.21	Seguridad del sistema. Los nodos de la solución deberán incorporar mecanismos de protección de datos, plataforma y ciclo de vida, cumpliendo como mínimo con lo siguiente: • Soportar cifrado y gestión de claves para la protección de datos en reposo, incluyendo administración de claves desde el subsistema de gestión o UEFI y soporte para unidades de autocifrado (SED) cuando la configuración de almacenamiento las incorpore. • Disponer de una función de borrado seguro de una sola acción para sanitización de medios y componentes soportados, conforme con las recomendaciones de NIST SP 800-88. • Contar con Trusted Platform Module (TPM) 2.0 integrado o embebido en la plataforma. • Soportar UEFI Secure Boot y mecanismos de arranque seguro que validen la integridad de los componentes durante el inicio del sistema. • Aceptar actualizaciones de componentes firmadas digitalmente y verificadas antes de su instalación, mitigando la ejecución de firmware no autorizado. • Contar con raíz de confianza inmutable basada en hardware y mecanismos de recuperación segura de firmware crítico hacia un estado conocido como válido. • Soportar mecanismos de seguridad física y de configuración tales como control de interfaces USB, bloqueo de configuración y detección de intrusión de chasis, de acuerdo con las capacidades de la plataforma ofertada. • El fabricante deberá documentar controles de seguridad aplicados a la cadena de suministro y al ciclo de vida del servidor, orientados a detectar o mitigar microcódigo malicioso, componentes falsificados o alteraciones no autorizadas.
1.22	Cumplimiento de estándares de industria. Los nodos ofertados deberán soportar y acreditar mediante documentación oficial del fabricante, según aplique, como mínimo los siguientes estándares, protocolos y

	capacidades: • ACPI 6.5; PCI Express 5.0; Wake on LAN (WOL); certificaciones Microsoft aplicables; PXE; USB 3.2 Gen 1; UEFI Clase 3; TPM 2.0; ENERGY STAR; SMBIOS 3.7. • Redfish API; IPMI 2.0; Advanced Encryption Standard (AES); SNMP v3; TLS 1.2 o superior; DMTF Redfish para administración de claves de Secure Boot; integración con Active Directory; y compatibilidad con condiciones ASHRAE A3/A4. • El fabricante deberá documentar cumplimiento o alineación aplicable con FIPS 140-3, NIST SP 800-53, NIST SP 800-171 y NIST SP 800-88 para las funciones de seguridad correspondientes.
2.	**INFRAESTRUCTURA DE CONECTIVIDAD (SWITCH DE TRANSFERENCIA DE RACK HÍBRIDO INTELIGENTE)**
2.1	Suministro de switch de transferencia de rack híbrido inteligente, como componente de soporte de la solución de infraestructura de backup, orientado a garantizar la continuidad operativa y la disponibilidad de los equipos que conforman la solución.
2.2	De acuerdo con los requerimientos técnicos establecidos en el Ítem 2.2.3 de la Ficha Técnica No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00, el equipo deberá cumplir con las características definidas en los numerales **2.2.3.1 al 2.2.3.27.** El proponente deberá tener en cuenta los numerales relacionados en el presente anexo de especificaciones técnicas adicionales, los cuales hacen parte integral del alcance técnico del suministro.
2.3	El oferente deberá presentar, como documento independiente de la oferta, un certificado emitido por el fabricante que certifique su condición de canal autorizado, así como la autorización para distribuir, instalar y brindar soporte a las soluciones y a los productos adquiridos.
2.4	Carta expedida por el fabricante del switch de transferencia de rack híbrido inteligente, con fecha de expedición no mayor a seis (6) meses, en la cual se indiquen claramente las referencias o números de parte y la descripción de los componentes ofertados. En dicha carta se deberá certificar que los equipos ofertados son originales, nuevos, de primer uso y no remanufacturados.
3.	**INFRAESTRUCTURA DE CONECTIVIDAD (SWITCH CORE 24 PUERTOS)**
3.1	El contratista deberá suministrar, instalar, configurar y poner en operación un (1) Switch Core Capa 3 para la infraestructura crítica de conectividad del DAVAA, garantizando alta disponibilidad, desempeño de nivel empresarial y cumplimiento integral del DOCUMENTO "No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03", el cual hace parte integral e indivisible del presente anexo técnico. El Switch Core de 24 puertos deberá cumplir como mínimo con lo siguiente:
3.2	Características de hardware, arquitectura de puertos, rendimiento, capacidad de procesamiento y componentes físicos del equipo, conforme a los numerales **3.3.1.2, 3.3.1.3, 3.3.1.4, 3.3.1.5, 3.3.1.6, 3.3.1.7, 3.3.1.8, 3.3.1.36, 3.3.1.37, 3.3.1.38 3.3.1.40** y 3.3.1.41 del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales establecen la configuración mínima de puertos (24 SFP+ 1G/10G, 12 RJ45 1G/2.5G/5G/10G Base-T y tarjeta 4 puertos 40/100Gbps QSFP/QSFP28), altura en rack, switching fabric, forwarding rate, capacidad de VLAN, soporte de jumbo frames, capacidad de stacking, puerto USB, buffer de memoria y fuentes de poder redundantes.
3.3	Requisitos relacionados con clasificación, priorización, políticas de calidad de servicio y control de congestión, conforme a los numerales **3.3.1.9, 3.3.1.10, 3.3.1.11, 3.3.1.12, 3.3.1.13, 3.3.1.14, 3.3.1.15, 3.3.1.34 y 3.3.1.35** del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales establecen colas de prioridad, clasificación wirespeed, QoS basado en políticas, remarcado extensivo, marcado DiffServ/IP Precedence y listas de control de acceso en capas 2, 3 y 4.
3.4	Cumplimiento de certificaciones, estándares IEEE, RFC y demás normativas técnicas, conforme a los numerales **3.3.1.16 y 3.3.1.17** del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales definen certificaciones eléctricas y de seguridad, estándares IEEE aplicables a Ethernet y autenticación, así como los RFC asociados a IPv4, IPv6, routing, multicast, gestión y seguridad.
3.5	Requisitos asociados a protocolos de enrutamiento dinámico, topologías redundantes y mecanismos de recuperación ante fallas, conforme a los numerales **3.3.1.22, 3.3.1.23, 3.3.1.24, 3.3.1.25, 3.3.1.26, 3.3.1.29,**

	3.3.1.30 Y 3.3.1.42 del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales establecen soporte de protocolos como OSPF, BGP, PIM, RIPng, compatibilidad con PVST+, stacking extendido, UDLD y soporte del protocolo G.8032 para anillos.
3.6	Características de seguridad, prevención de bucles, control de acceso y protección de enlaces, conforme a los numerales **3.3.1.19, 3.3.1.20, 3.3.1.21, 3.3.1.23, 3.3.1.31, 3.3.1.32, y 3.3.1.33** del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales establecen monitoreo de enlaces, detección de loops, control de MAC duplicadas, prevención de tormentas de broadcast, autenticación, soporte OpenFlow y VRF Lite.
3.7	Capacidades de administración local y remota, automatización, respaldo de configuraciones y mecanismos de eficiencia operativa, conforme a los numerales **3.3.1.18, 3.3.1.27, 3.3.1.28 y 3.3.1.43** del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, relacionados con gestión centralizada, scripting, ahorro energético y administración por CLI y Web.
3.8	Condiciones relacionadas con el suministro de módulos, cables y accesorios necesarios para la implementación, conforme a los numerales **3.3.1.4, 3.3.1.44 y 3.3.1.45** del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, incluyendo módulos SFP+, cables de stacking originales del fabricante y demás elementos requeridos para la correcta puesta en operación, sin incluir tendidos de fibra óptica.
3.9	Requisitos de garantía, soporte técnico y documentación de respaldo del fabricante, conforme a los numerales 3.2.3 y 3.2.3.1 del DOCUMENTO No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03, los cuales establecen garantía mínima de tres (3) años, soporte 7x24, reemplazo avanzado de partes, cartas de autorización del fabricante y certificación de ingeniero autorizado para la puesta en marcha.
4.	**INFRAESTRUCTURA DE CONECTIVIDAD (MANTENIMIENTO PREVENTIVO A PUNTO DE DATOS)**
4.1	El contratista deberá ejecutar actividades de mantenimiento preventivo para los puntos de datos del DAVAA, con el propósito de garantizar su adecuada operación, desempeño, identificación y correcta administración técnica dentro del sistema de telecomunicaciones. Las actividades deberán desarrollarse conforme a buenas prácticas de cableado estructurado y deberán incluir como mínimo lo siguiente:
4.2	Verificación del estado físico de jacks, faceplates, módulos, conectores y elementos asociados, identificando posibles daños o deterioros que afecten la conectividad.
4.3	Revisión, ajuste y actualización de la identificación del punto tanto en el puesto de trabajo como en el patch panel correspondiente, asegurando coherencia y trazabilidad.
4.4	Levantamiento y validación del mapeo físico del punto, identificando origen y destino (patch panel – puesto de trabajo), puerto asociado y estado operativo.
4.5	Ejecución de reponchado cuando se evidencien fallas derivadas de mala terminación, falso contacto o deterioro en la conexión.
4.6	En caso de evidenciar deterioro o daño, se deberá realizar el reemplazo del jack, módulo o faceplate correspondiente para restablecer condiciones adecuadas de funcionamiento. No incluye reemplazo de cableado horizontal.
4.7	Cuando las necesidades operativas lo requieran y el cableado existente lo permita, se podrá realizar la reubicación del punto dentro del mismo espacio físico, hasta una distancia máxima de ocho (8) metros, garantizando su correcta fijación y operatividad.
4.8	Peinado y organización de los elementos visibles del punto y sus conexiones asociadas, respetando radios de curvatura y buenas prácticas técnicas.
4.9	Ejecución de pruebas de verificación o certificación del punto intervenido, garantizando el cumplimiento de los parámetros técnicos aplicables.
4.10	Actualización del registro técnico correspondiente a los puntos intervenidos, incluyendo ajustes, correcciones o cambios realizados.
4.11	Las actividades deberán ejecutarse en coordinación con el personal designado por el DAVAA, minimizando impactos en la operación. Al finalizar, el contratista deberá entregar informe técnico que relacione los puntos

5.	INFRAESTRUCTURA DE CONECTIVIDAD (INSTALACIÓN DE PUNTO DE DATOS CATEGORÍA 6ª)
5.1	El contratista deberá ejecutar el suministro, instalación, certificación y puesta en funcionamiento de puntos de datos categoría 6A en tecnología U/UTP, como parte del fortalecimiento de la infraestructura crítica de conectividad del DAVAA, garantizando su correcto desempeño y el cumplimiento de los parámetros técnicos definidos en el presente anexo.
5.2	El proponente deberá incluir todos los elementos, materiales, componentes y labores necesarias para asegurar que los puntos de datos instalados queden completamente funcionales en todos sus aspectos a nivel de infraestructura de telecomunicaciones.
5.3	Las actividades comprenderán la adquisición, suministro, instalación, organización, identificación, certificación y puesta en funcionamiento de los componentes de la infraestructura de red en cobre requeridos para la implementación de los puntos de datos conforme a los numerales **4.2, 4.3, 4.4, 4.5, 4.6 y 4.7** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 los cuales establecen las características y condiciones mínimas para jacks de puesto de trabajo, plugs de terminación en campo, patch panel, organizadores, patch cords y lineamientos asociados a solución monomarca.
5.4	Se deberá realizar el suministro e instalación de enlaces de datos en par trenzado de cobre categoría 6A tipo U/UTP, que cumplan con los estándares internacionales ANSI/TIA-568 en sus últimas versiones, ISO/IEC 11801 Clase EA y el estándar IEEE 802.3an-2006, para requerimientos de canal que soporten aplicaciones 10GBASE-T, conforme al numeral **4.1** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 el cual define condiciones mínimas para el subsistema de cableado horizontal y administración, incluyendo desempeño para 10G, PoE y condiciones generales de operación del enlace.
5.5	Se deberá contemplar el suministro e instalación de los sistemas y componentes de organización, identificación y marcación de la infraestructura de red en cobre, conforme al estándar internacional ANSI/TIA-606-C, conforme a los numerales **4.4 y 4.5** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 los cuales contemplan criterios mínimos para instalación en gabinetes, administración posterior, identificación/etiquetado y ordenamiento del sistema mediante organizadores.
5.6	Se deberá realizar la entrega de informes de certificación de la infraestructura de red para cada uno de los enlaces de cobre instalados, así como de los componentes cuando aplique certificación de canal, conforme al numeral **4.9** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 el cual establece la entrega del soporte documental de certificación en desempeño para los puntos de datos.
5.7	Los componentes físicos de la infraestructura (cable, patch cords, patch panels, organizadores, entre otros) deberán seleccionarse con base en las premisas del estándar ANSI/TIA-568, ISO/IEC 11801 y demás estándares ANSI/TIA aplicables para edificaciones comerciales, conforme al numeral **4.7** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 aplicable a los elementos que conforman la conectividad pasiva del sistema.
5.8	El oferente deberá realizar la entrega de fichas técnicas obligatorias, conforme al numeral **4.8** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 el cual exige adjuntar fichas técnicas como soporte de cumplimiento y validación.
5.9	El oferente deberá adjuntar a su oferta, acreditación como canal autorizado para distribución/instalación/garantía: conforme al numeral **4.10** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 el cual requiere carta/certificación del fabricante indicando la capacidad del oferente para distribuir, instalar y extender garantía de la conectividad pasiva.
5.10	El contratista deberá cumplir con los requisitos de canalización/tubería perimetral, conforme al numeral **4.11** del DOCUMENTO No. JEMPP-CEDE4-DIETE-ET-04860/COMUN-01 aplicable únicamente cuando el alcance del contrato incluya suministro e instalación de canalización a la vista u oculta para la implementación de los puntos de datos.
6.	**INFRAESTRUCTURA DE CONECTIVIDAD (INSTALACIÓN DE PUNTO ELÉCTRICO DOBLE)**
6.1	El contratista deberá ejecutar el suministro, instalación, conexión, verificación y puesta en funcionamiento de puntos eléctricos dobles (normal y regulado, cuando aplique), requeridos para soportar la operación de la infraestructura crítica de conectividad y respaldo tecnológico del DAVAA, garantizando condiciones de

	seguridad eléctrica, continuidad operativa, calidad de la instalación y cumplimiento normativo.
6.2	La ejecución de las actividades deberá realizarse en estricto cumplimiento de la normatividad vigente aplicable, incluyendo como mínimo el Reglamento Técnico de Instalaciones Eléctricas (RETIE), la NTC 2050 (Código Eléctrico Colombiano) y demás normas técnicas, reglamentos, códigos y buenas prácticas que regulen el diseño, instalación y verificación de instalaciones eléctricas de baja tensión en Colombia, así como las disposiciones de seguridad industrial y prevención del riesgo eléctrico aplicables al sitio de intervención.
6.3	El contratista deberá garantizar que la instalación se ejecute con materiales certificados, procedimientos adecuados y personal idóneo, asegurando: correcta polaridad, continuidad del conductor de protección (puesta a tierra), adecuada canalización y fijación, identificación/rotulado cuando aplique, y ausencia de condiciones que generen riesgo para personas o equipos.
6.4	Como parte del cierre de la actividad, el contratista deberá realizar las pruebas y verificaciones funcionales y de seguridad que correspondan, y entregar a la Entidad el soporte documental de ejecución (registro de intervención, evidencias y resultados de pruebas), de manera que se garantice trazabilidad y aceptación técnica del suministro e instalación.
7.	**INFRAESTRUCTURA DE CONECTIVIDAD (MANTENIMIENTO PREVENTIVO DE RACK DE COMUNICACIONES)**
7.1	El contratista deberá ejecutar el servicio de mantenimiento preventivo sobre los racks o gabinetes de telecomunicaciones que conforman la infraestructura tecnológica del DAVAA, con el propósito de garantizar su integridad estructural, adecuada organización interna, seguridad física y condiciones óptimas para la operación continua de los equipos instalados. Las actividades deberán desarrollarse conforme a las buenas prácticas de cableado estructurado y bajo coordinación con el personal designado por la Entidad.
7.2	Durante la ejecución contractual, el contratista deberá realizar como mínimo una (1) jornada de mantenimiento preventivo por cada rack incluido en el alcance, desarrollando las siguientes actividades:
7.2.1	Verificación visual de la estructura metálica del gabinete, identificando posibles deformaciones, deterioro, desgaste o condiciones que puedan comprometer su estabilidad.
7.2.2	Revisión del estado de bandejas, rieles, paneles laterales, puertas y demás componentes estructurales.
7.2.3	Validación del sistema de anclaje al piso o pared, comprobando ausencia de movimientos anormales o vibraciones.
7.2.4	Inspección superficial para detectar signos visibles de corrosión o afectación del recubrimiento.
7.2.5	Reorganización y peinado del cableado de cobre y fibra óptica contenido en el rack, garantizando radios de curvatura adecuados y ausencia de tensión mecánica.
7.2.6	Verificación de que los cables no se encuentren presionados por puertas, paneles u otros elementos del gabinete o rack.
7.2.7	Ajuste de organizadores horizontales y verticales existentes, optimizando la distribución interna del cableado.
7.2.8	Verificación y ajuste de la marcación existente en patch cords, enlaces y puertos, conforme al esquema de administración definido por el DAVAA.
7.2.9	Levantamiento y validación de la información asociada al rack, incluyendo identificación de patch panels, equipos instalados y puertos activos.
7.2.10	Limpieza interna y externa del rack, retirando polvo y residuos que puedan afectar la ventilación y el desempeño de los equipos.
7.2.11	Verificación visual del estado general de conectores, paneles y elementos de interconexión, sin realizar intervenciones de configuración.
7.2.12	Revisión del ajuste de tornillería y soportes visibles de los equipos instalados.
7.3	Las actividades deberán ejecutarse en ventanas previamente coordinadas con el DAVAA, minimizando cualquier impacto sobre la operación. El mantenimiento preventivo no incluye suministro ni reemplazo de componentes estructurales, accesorios o

	elementos de cableado, salvo que estos se encuentren expresamente contemplados en el alcance contractual.
8.	**MANTENIMIENTO PREVENTIVO DE SWITCHES DE RED**
8.1	El contratista deberá ejecutar el servicio de mantenimiento preventivo sobre los switches de red incluidos en el alcance contractual, con el propósito de preservar condiciones óptimas de operación, organización física, trazabilidad de conexiones y continuidad del servicio en la infraestructura tecnológica del DAVAA.
8.2	Durante la ejecución contractual, el contratista deberá realizar como mínimo una (1) jornada de mantenimiento preventivo por cada equipo incluido, desarrollando las siguientes actividades técnicas:
8.2.1	Verificación visual del estado físico del equipo, incluyendo chasis, módulos, puertos, ventiladores, conectores, indicadores luminosos y elementos de fijación, identificando posibles anomalías o condiciones que puedan afectar la operación.
8.2.2	Limpieza externa e interna mediante el uso de herramientas y elementos apropiados para entornos de telecomunicaciones, tales como aire comprimido controlado y equipos antiestáticos, evitando afectaciones a los componentes electrónicos.
8.2.3	Revisión y aseguramiento de cables de energía y datos asociados al equipo (patch cords, conectores y enlaces), validando correcta inserción, sujeción y estado físico.
8.2.4	Organización, peinado y redistribución de los cables de interconexión, utilizando los organizadores existentes en el rack y respetando radios de curvatura, evitando tensiones mecánicas, cruces indebidos u obstrucciones que afecten ventilación o mantenimiento futuro.
8.2.5	Marcación y/o actualización de etiquetas en patch cords y puertos intervenidos, en ambos extremos, conforme al esquema de identificación vigente del DAVAA, garantizando trazabilidad y control técnico.
8.2.6	Registro actualizado de las interconexiones físicas del equipo (equipo origen–puerto / equipo destino–puerto), incluyendo ubicación en rack (gabinete y unidad U), con observaciones relevantes para la gestión de la red.
8.2.7	Revisión visual del estado funcional del equipo, validando indicadores de operación, ventilación y posibles alarmas visibles, sin realizar modificaciones en la configuración.
8.2.8	Ejecución de pruebas técnicas básicas, tales como verificación de enlaces físicos activos/inactivos y validaciones simples de conectividad, siempre dentro de los accesos autorizados por el personal designado por el DAVAA.
8.3	Las actividades deberán ejecutarse en ventanas de mantenimiento previamente coordinadas con el DAVAA, minimizando cualquier impacto sobre la operación. Cualquier intervención sobre enlaces críticos deberá contar con validación y autorización del personal designado por la Entidad. El mantenimiento preventivo no incluye cambios de configuración, actualización de firmware ni modificaciones lógicas.
	EQUIPO DE TRABAJO El oferente deberá disponer del personal suficiente, idóneo y debidamente certificado para la instalación, configuración, integración, puesta en funcionamiento y soporte técnico asociado de los equipos objeto de la presente especificación técnica, garantizando la correcta ejecución del alcance contractual. **1. Director Técnico de Implementación** **Formación académica:** • Profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica, Eléctrica o afines (SNIES). • Posgrado en Dirección o Gestión de Proyectos. **Responsabilidad general:** Liderar la ejecución técnica del proyecto y asegurar el cumplimiento de alcance, cronograma y calidad. **Responsabilidades específicas:** • Planificar y supervisar el despliegue técnico. • Coordinar equipos y validar entregables. • Controlar hitos, riesgos y avances.

Certificaciones obligatorias (vigentes):

- PMP.
- ITIL v3 o superior.
- Certificación en seguridad.

2. Especialista en Arquitectura y Seguridad de Infraestructura
Formación académica:

- Profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica, Eléctrica o afines (SNIES).
- Posgrado en Seguridad o Redes.

Responsabilidad general:

- Diseñar y asegurar la arquitectura de red y seguridad del proyecto.
- Responsabilidades específicas:
- Configurar y asegurar equipos activos.
- Implementar controles de seguridad.
- Validar cumplimiento técnico.

Certificaciones obligatorias:

- CompTIA Security+ vigente.
- Certificación profesional en Seguridad de Redes.
- Certificación o formación en Arquitectura de Redes.
- Certificación nivel experto en la tecnología del switch ofertado.

3. Especialista en Respaldo y Continuidad Tecnológica
Formación académica:

- Profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica, Eléctrica o afines (SNIES).

Responsabilidad general:

- Implementar y asegurar la operación inicial de la solución de backup.

Responsabilidades específicas:

- Configurar la solución de respaldo.
- Ejecutar pruebas de recuperación.
- Integrar con monitoreo y documentar la implementación.

Certificaciones obligatorias:

- Certificación profesional en la solución de backup ofertada.
- CompTIA Server+ vigente.
- CompTIA Linux+ vigente.
- Certificación técnica en monitoreo eléctrico y ambiental de la marca del interruptor de transferencia ofertado.

Para la acreditación de la Formación Académica, el proponente deberá adjuntar copia de los diplomas correspondientes a los estudios cursados en los niveles de pregrado, posgrado y a las certificaciones exigidas. En el caso de certificaciones que cuenten con fecha de vencimiento, estas deberán encontrarse vigentes tanto al momento de la evaluación del proceso como durante la ejecución del contrato.

La Experiencia Específica se acreditará mediante la presentación, junto con la oferta, de certificaciones laborales o contractuales que contengan como mínimo la fecha de inicio, la fecha de terminación, la descripción de las actividades desarrolladas y la identificación completa de quien expide la certificación, incluyendo firma, nombre, dirección y teléfono. Adicionalmente, deberá anexarse la hoja de vida, copia de la matrícula o tarjeta profesional vigente —según aplique— expedida por el Consejo Profesional correspondiente, así como copia de la cédula de ciudadanía.

	Igualmente, se deberá aportar el certificado de antecedentes y vigencia expedido por el consejo profesional respectivo para los profesionales a los que aplique. Todos los documentos deberán presentarse en copias escaneadas, claras y legibles. Así mismo, se deberá adjuntar la carta de compromiso del personal mínimo requerido, suscrita por el representante legal, junto con la carta de autorización para la presentación de la hoja de vida y el compromiso de vinculación con el proponente, firmada por cada uno de los profesionales y técnicos ofertados. **Nota:** - El supervisor evaluará el desempeño laboral del personal asignado para los mantenimientos preventivos y/o correctivos, 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 División de Aviación Asalto Aéreo – DAVAA. serán asumidos por el adjudicatario quién debe repararlos sin costo alguno o hacer reposición por equipos o elementos de iguales o mejores características.

Respetuosamente,

Teniente Coronel NESTOR ANDRES ARDILA CAVIEDES
Gerente del Proyecto

Elaboró: TE. Cindy Hernández
Comité Estructurador