ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
1.	**ALMACENAMIENTO TIPO SAN/NAS**			
1.1.	Marca	<<*Especificar*>>		
1.2.	Modelo	<<*Especificar*>>		
1.3.	Cantidad	Un (01) sistema de almacenamiento SAN/NAS		
1.4.	Ubicación	El sistema de almacenamiento SAN/NAS se instalará en la siguiente dirección: • 01 (un) sistema de almacenamiento ubicado en el centro procesamiento de datos principal, en las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones -OFTIC, carrera 59 #26-21, CAN, Bogotá D.C.		
ARQUITECTURA Y GENERALIDADES				
1.5.	Requerimiento	El sistema de almacenamiento unificado (bloque, archivo y objetos) de arquitectura All-Flash, basado en discos SSD NVMe. Cada sistema debe contar con mínimo dos (2) en configuración Activo-Activo. Debe soportar de forma nativa y simultánea los protocolos SAN (Fibre Channel, iSCSI), Objetos (S3) y NAS (NFS, SMB, CIFS).		
1.6.	Catalogación empresarial	Los equipos de almacenamiento ofertados deberán pertenecer a una familia de productos clasificada como Enterprise-Class para grandes centros de datos por el fabricante, y cuyo fabricante haya sido reconocido como Líder (Leaders Quadrant) en el Gartner® Magic Quadrant™ para Plataformas de Almacenamiento Empresarial (Enterprise Storage Platforms) en la edición más reciente disponible.		
1.7.	Arquitectura general	El dispositivo debe incluir licenciamiento para almacenamiento tipo SAN, NAS y S3.		
1.8.	Arquitectura física	Sistemas unificados nativos, sin gateways ni componentes virtuales adicionales, no se aceptarán almacenamientos gestionados por software		
1.9.	Fecha de fabricación	Se deberá garantizar que los equipos entregados son nuevos, de última tecnología, no remanufacturados y fabricados en 2026		
1.10.	Fecha de lanzamiento del producto	Los equipos de almacenamiento ofertados deben corresponder a una generación de producto lanzada comercialmente a partir del año 2025, incorporando los avances tecnológicos más recientes en arquitectura NVMe, inteligencia artificial para gestión de I/O y protección contra ransomware de última generación. No se aceptarán sistemas basados en arquitecturas lanzadas con anterioridad al año 2024, aunque hayan sido fabricados en fechas posteriores.		
1.11.	Unidades de Rack	El sistema de almacenamiento no debe superar las cuatro (4) unidades de rack.		
CAPACIDAD Y ALMACENAMIENTO				
1.12.	Capacidad Nativa	El sistema de almacenamiento deberá ser entregado con una capacidad mínima de 512 TB usables después de la configuración del arreglo de discos en RAID 6 (o protección equivalente N+2), sin aplicar algoritmos de compresión ni deduplicación. La solución debe ser All-Flash con discos SSD NVMe.		
1.13.	Crecimiento	Cada sistema debe tener capacidad de crecimiento mínimo de 1 PB usables o superior, tanto en controladoras nuevas (scale-out) como en capacidad de discos (scale-up) y debe soportar una expansión de hasta 8 controladoras garantizando la inversión a futuro.		
1.14.	Plan de crecimiento a tres años	Se deberá entregar, como parte de los documentos de cierre del proyecto, un plan de crecimiento del sistema de almacenamiento para los próximos 3 (tres) años, considerando el crecimiento estimado de datos de la Oficina de Tecnologías de la Información y las Comunicaciones. El documento deberá incluir: • Procedimientos detallados para agregar capacidad mediante adición de discos (scale-up) o incorporación de nuevas controladoras (scale-out) • Compatibilidad verificada con futuras versiones de hardware y software del fabricante, en el marco de la garantía de actualización sin migración de datos ofrecida por el fabricante; y estimación de costos aproximados por cada opción de expansión.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
		• Este documento deberá ser avalado por el fabricante o su representante oficial en Colombia.		
1.15.	Thin Provisioning	Cada sistema de almacenamiento deberá soportar aprovisionamiento delgado (thin provisioning) nativo, permitiendo la creación de volúmenes lógicos con capacidad superior al almacenamiento físico disponible actualmente, asignando espacio físico únicamente a medida que los datos son escritos		
1.16.	Eficiencia de Almacenamiento	Además de la capacidad nativa, cada sistema de almacenamiento unificado debe incluir tecnologías de deduplicación y compresión en línea (en caliente) que operen sin afectar el rendimiento.		
1.17.	Gestión del ciclo de vida de los datos (ILM)	Cada sistema debe soportar políticas automatizadas de gestión del ciclo de vida de los datos (Information Lifecycle Management ILM), incluyendo: • Movimiento automático de datos entre niveles de almacenamiento (tiers) basado en frecuencia de acceso y antigüedad, mediante la funcionalidad nativa de tiering automático del fabricante • Archivado de datos históricos hacia repositorios de largo plazo mediante la funcionalidad nativa de movilidad y archivado de datos del fabricante • Eliminación automática de datos que hayan cumplido su período de retención definido por el administrador; y mecanismos de protección contra eliminación accidental de datos críticos mediante la funcionalidad nativa de bloqueo e inmutabilidad de datos del fabricante. • Todas estas funcionalidades deberán estar licenciadas a perpetuidad en ambos sistemas. • El contratista deberá configurar y documentar las políticas de ILM implementadas, incluyendo los flujos de movimiento de datos entre tiers y los reportes de optimización de almacenamiento obtenidos.		
1.18.	Desgaste de discos	Cada sistema de almacenamiento debe incluir algoritmos de nivelación de desgaste del disco y anti desgaste, reportando su estado actual en la interfaz de gestión del equipo.		
1.19.	Distribución de capacidad.	Cada sistema de almacenamiento para cada sitio tener una capacidad mínima usable de 512 TB.		
1.20.	Protección de Datos	Cada sistema debe admitir RAID 6 y una configuración RAID-TP que pueda tolerar fallas de hasta tres discos simultáneamente, excluyendo discos de repuestos en caliente.		
RENDIMIENTO				
1.21.	Memoria caché	Cada sistema deberá ser entregado con un mínimo de 1TB de memoria caché por sistema (no por controladora). No se acepta el uso de discos SSD, tecnologías híbridas o memoria virtual para cumplir este requisito.		
1.22.	Núcleos de procesamiento	Cada sistema de almacenamiento deberá contar mínimo dos CPU de 64 núcleos de procesamiento por controladora.		
1.23.	Interconexión Back-End de alta velocidad	Cada sistema debe utilizar un protocolo de interconexión back-end de al menos 100 Gbps RDMA entre controladoras y enclosures de discos. Esta arquitectura garantiza que la interconexión interna no sea cuello de botella, asegurando latencias de acceso de hasta 0,05 ms extremo a extremo (E2E NVMe).		
1.24.	Tiempo máximo de reconstrucción RAID	Ante la falla de un SSD, cada sistema debe reconstruir hasta 1 TB de datos en un tiempo máximo de 15 (quince) minutos, utilizando procesamiento inteligente distribuido entre el enclosure de discos y el de controladoras, sin impacto significativo en las operaciones en producción durante la reconstrucción.		
1.25.	Tiempo máximo de conmutación activo-activo	El sistema activo-activo debe completar la conmutación automática ante cualquier falla de controladora o de enlace de replicación en un tiempo máximo de 2 (dos) segundos, sin interrupción del servicio a los hosts conectados ni intervención del administrador.		
CONECTIVIDAD Y PROTOCOLOS				
1.26.	Host Ports	**Puertos Front-End (Host Ports):** el sistema de almacenamiento deberá incluir un mínimo de 24 (veinticuatro) puertos front-end de alta velocidad, activos, funcionales y licenciados, que podrán ser utilizados de manera flexible para		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
		conectividad SAN (Fibre Channel) o LAN (Ethernet). La distribución y tipo de puerto deberá cumplir con lo siguiente: Mínimo 8 (ocho) puertos de 32 Gbps Fibre Channel (FC) para conectividad SAN. Mínimo 8 (ocho) puertos de 25 GbE (Ethernet) para conectividad LAN NAS. Mínimo 8 (ocho) puertos de 25 GbE (Ethernet) para conectividad LAN Objetos. Los puertos de 25 GbE deberán soportar los protocolos necesarios para servicio NAS y para replicación de datos basada en almacenamiento. No se requiere un juego de puertos exclusivos y separados para replicación; los puertos de 25 GbE podrán compartir el tráfico de servicio y replicación de manera segura y eficiente. Adicionalmente, se requieren 2 (dos) puertos de cobre a 1 GbE dedicados exclusivamente para la administración out-of-band de cada sistema. Todos los puertos deben estar activos, certificados y licenciados con sus correspondientes módulos SFP28 en origen y destino. Los switches instalados en el centro de procesamiento de datos principal de la Policía Nacional son de marca “Nexus 93180YC-Los puertos requeridos deben ser administrables, auto negociables, estar activos, funcionales y licenciados con sus respectivos módulos SFP28 en origen y destino. Los switches instalados en el centro de procesamiento de datos principal de la Policía Nacional son de marca “Nexus 93180YC-EX bundle PID”, por tal motivo el contratista debe entregar para el caso del destino los SFP originales de marca “Cisco SFP-25G-SR-S 25GBASE-SR” para asegurar la compatibilidad		
1.27.	Puertos FC-NVMe y NVMe over RoCE	Los puertos front-end de cada sistema deben soportar, además de FC y Ethernet tradicionales, los protocolos FC-NVMe (Fibre Channel sobre NVMe) y NVMe over RoCE (RDMA over Converged Ethernet), garantizando conectividad de ultrabaja latencia. Cada sistema deberá soportar velocidades de 8/16/32/64 Gbps en FC/FC-NVMe y 10/25/40/100 GbE para Ethernet, asegurando compatibilidad con infraestructura actual y futura.		
1.28.	Modulos I/O y densidad de puertos	Cada enclosure de controladoras debe soportar un mínimo de 28 módulos I/O intercambiables en caliente (hot-swappable), con capacidad para alojar hasta 96 puertos front-end por enclosure de controladoras. Esta densidad garantiza que los puertos mínimos exigidos puedan instalarse con margen de crecimiento sin requerir hardware adicional.		
1.29.	Compatibilidad con Switches SAN Fibre Channel	Cada sistema de almacenamiento debe ser compatible e interoperable con switches SAN Fibre Channel de fabricantes líderes del mercado, incluyendo como mínimo los siguientes modelos certificados: Brocade G620 (32 Gbps, hasta 64 puertos), Brocade G630 (32 Gbps, hasta 128 puertos), Brocade G720 (64 Gbps, hasta 96 puertos), Brocade G730 (64 Gbps, hasta 96 puertos).		
1.30.	Soporte de protocolo	Cada sistema debe soportar mínimo iSCSI, S3, CIFS/SMBv3, NFSv4.1, Fibre Channel y NDMP.		
1.31.	Conectividad de los servidores	Los servidores de aplicación virtual y físicos deben conectarse al almacenamiento SAN/NAS/Objetos a través de puertos asignados en los switches que le permita conectividad al almacenamiento por medio de la red LAN y FC.		
1.32.	Capacidad de conectividad SAN	Cada sistema de almacenamiento ofertado debe tener la capacidad de trabajar y dar servicio en red SAN de manera concurrente, garantizando que todos los hosts conectados puedan acceder simultáneamente a sus volúmenes asignados sin degradación de rendimiento.		
1.33.	Sistema Operativo Soportado	Cada sistema debe ser compatible con las siguientes versiones o superiores: Microsoft Windows Server 2012/2016/2019/2022/2025, Oracle Linux 7/8/9, Red Hat Enterprise Linux 7, garantizando capacidad de archivado e integración con servidores virtuales y datos no estructurados. La compatibilidad debe incluir tanto arquitecturas de 64 bits en servidores físicos como en entornos virtualizados, con soporte de los protocolos SAN (FC, iSCSI) y NAS (NFS, CIFS/SMB) desde cada sistema operativo listado.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
1.34.	Compatibilidad con Ambientes de Virtualizacion	Cada sistema de almacenamiento debe ser compatible y estar certificado con los principales ambientes de virtualización del mercado, siempre que el acceso al almacenamiento se realice mediante protocolos estándar de la industria incluyendo como mínimo: VMware vSphere ESXi (versiones 7.0 y 8.0 o superiores) con soporte de VMware VAAI, VASA, VVols 2.0, integración con VMware Site Recovery Manager (SRM) mediante plugin SRA del fabricante, y soporte de multipath mediante driver nativo del fabricante o VMware NMP/HPP; Microsoft Hyper-V (Windows Server 2016, 2019 y 2022 o superiores); Red Hat Enterprise Linux (RHEL) con soporte en entornos KVM, Red Hat OpenStack Platform (versiones 16.x y 17.x o superiores) y Red Hat OpenShift como almacenamiento persistente para contenedores vía CSI Driver; Citrix XenServer; Oracle VM for x86; IBM AIX e IBM VIOS; SUSE Linux Enterprise Server; y Kubernetes mediante Container Storage Interface (CSI) nativo del fabricante para aprovisionamiento dinámico de volúmenes persistentes.		
SERVICIOS DE DATOS NAS/SAN				
1.35.	Compartir archivos entre plataformas NAS	El sistema de almacenamiento admite el acceso entre protocolos (NFS y CIFS) a los sistemas de archivos sin pérdida de permisos de acceso. Admite cuatro estilos de seguridad para el acceso multiprotocolo: NTFS, UNIX, MIX y NATIVE.		
1.36.	Protección Nativa Contra Ransomware	Cada sistema de almacenamiento ofertado (tanto el principal como el de contingencia) deberá contar con capacidades nativas de prevención, detección y recuperación frente a ataques de ransomware, sin depender exclusivamente de software externo. Estas capacidades deberán estar licenciadas perpetuamente integradas de fábrica en la solución de almacenamiento y operativas desde el momento de la puesta en marcha.		
1.37.	Interoperabilidad entre protocolos S3 y NAS	Los servicios de archivos y objetos pueden habilitarse en el mismo espacio de nombres en el mismo grupo de almacenamiento al mismo tiempo. Los protocolos de acceso como NFS, CIFS y S3 pueden configurarse para acceder al mismo archivo en el mismo grupo de almacenamiento. Un solo archivo puede escribirse a través del protocolo de objetos S3 (o NAS) y leerse a través de NAS (o el protocolo de objetos S3).		
1.38.	Convergencia NAS y S3 en misma instancia sin conversión	La convergencia entre los protocolos NAS (NFS, CIFS/SMB) y S3 debe operar sobre la misma instancia de almacenamiento y espacio de nombres, sin necesidad de copias intermedias ni conversión de datos. Un archivo escrito mediante S3 debe poder leerse directamente mediante NFS o CIFS (y viceversa), garantizando coherencia de datos y permisos en tiempo real.		
1.39.	Cuota de almacenamiento NAS	Cada sistema de almacenamiento deberá incluir la capacidad de implementar cuotas de almacenamiento para usuarios. Las cuotas deberán ser implementadas a través de políticas definidas por el administrador, aplicables a cualquier usuario configurado en el gestor de usuarios de la entidad (LDAP y Active Directory).		
1.40.	Balanceo de carga	Cada sistema de almacenamiento SAN/NAS/Objetos debe estar en capacidad de balancear en línea la información a través de todos los nodos/controladores o de los nodos/controladores agrupados, sin impactar el acceso a los archivos por parte de los usuarios.		
1.41.	Soporte de multitenencia lógica	Cada sistema debe soportar multitenencia lógica segura (multi-tenant), permitiendo entornos de almacenamiento lógicamente aislados para diferentes dependencias o unidades organizativas. Cada entorno debe tener políticas independientes de capacidad, rendimiento (QoS), acceso y auditoría, gestionados desde una consola administrativa unificada.		
1.42.	QoS por carga de trabajo crítica	El contratista deberá configurar políticas de Calidad de Servicio (QoS) por carga de trabajo en cada sistema de almacenamiento, estableciendo para los grupos de discos o LUNs asociados a las bases de datos del SECAD.		
DISPONIBILIDAD Y CONTINUIDAD DEL NEGOCIO				
1.43.	Alta Disponibilidad y Resiliencia	Cada sistema debe garantizar 99,9999% de disponibilidad, soporte Hot-Swap de componentes, snapshots programados y replicación entre ambos almacenamientos.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
		Cada sistema deberá garantizar la integridad de los datos y mantener la continuidad del servicio durante el proceso de intercambio, con una interfaz de gestión que permita supervisar y controlar este procedimiento de forma segura.		
1.44.	Controladoras	Cada sistema debe contar con un mínimo de dos (dos) controladoras en configuración activo-activo, que trabajen en paralelo para el procesamiento de todas las operaciones de entrada/salida (I/O). Las controladoras deben garantizar alta disponibilidad, de manera que, ante el fallo de una de ellas, la otra asuma la totalidad de la carga de forma automática y sin interrupción del servicio tanto en SAN, NAS y S3. La arquitectura debe permitir crecimiento futuro en capacidad y rendimiento, soportando escalamiento horizontal (scale-out) y vertical (scale-up), según la arquitectura nativa del fabricante. La arquitectura debe ser capaz de tolerar la falla de una controladora sin interrupción del servicio o impacto en la disponibilidad de datos.		
1.45.	Componentes redundantes	Cada solución de almacenamiento físico debe tener controladores intercambiables en caliente redundantes, fuentes de alimentación, ventiladores e interfaces de host front-end		
1.46.	Replicación SAN y NAS	La solución de almacenamiento deberá incluir capacidades avanzadas de replicación remota para entornos SAN y NAS, cumpliendo como mínimo con los siguientes requerimientos: • Replicación remota síncrona a nivel de bloque (SAN). • Replicación remota asíncrona a nivel de bloque (SAN). • Capacidad de replicación de instantáneas (snapshots) desde el sitio primario al secundario (SAN). • Posibilidad de restauración de datos directamente desde el sitio secundario (SAN). • Compresión de datos en los enlaces de replicación para optimizar el uso del ancho de banda (SAN). • Replicación remota asíncrona a nivel de sistema de archivos (NAS). • Replicación de datos entre sistemas de archivos locales y remotos (NAS).		
1.47.	WORM y Snapshots	Cada sistema debe soportar WORM y Snapshots con un mínimo de 6.400 snapshots simultáneos por sistema, con capacidad de crear al menos un snapshot por LUN/volumen activo sin degradación del rendimiento. Cada sistema deberá soportar la creación de snapshots mediante la funcionalidad nativa o equivalente del fabricante, con una frecuencia mínima de captura de tres (3) segundos para snapshots periódicos, aplicable tanto a entornos SAN como NAS.		
SEGURIDAD				
1.48.	Seguridad y protección	Ambos sistemas deben incluir: • Detección anti-ransomware nativa deberá garantizar una tasa de detección mínima del 99,99%, con capacidad de intercepción pre-evento, detección en tiempo real durante el evento, e identificación post-evento, cubriendo tanto entornos SAN como NAS. • inmutabilidad de los datos. • doble factor de autenticación. • RBAC. • soporte AD/LDAP y auditoría de archivos CIFS/NFS.		
1.49.	Alertas de seguridad y detección de actividad sospechosa	Cada sistema deberá generar alertas automáticas en tiempo real ante eventos de seguridad anómalos, incluyendo como mínimo: intentos de inicio de sesión fallidos de forma repetida, accesos fuera del horario o desde ubicaciones no autorizadas, modificaciones no autorizadas de configuración del sistema, y patrones de I/O inusuales que puedan indicar un ataque de ransomware en curso. Estas alertas deberán ser notificadas al administrador mediante correo electrónico, protocolo SNMP y/o integración con plataformas de monitoreo SIEM. La funcionalidad de detección y análisis de ransomware nativa del		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
		fabricante deberá estar licenciada, activa y configurada desde la entrega de ambos sistemas.		
1.50.	Cumplimiento normativo y seguridad ampliada	Adicionalmente a los requisitos de seguridad básicos, cada sistema deberá incluir los siguientes mecanismos: • Validación de integridad del contenido almacenado mediante funciones HASH con detección y reparación automática de corrupción silenciosa de datos (silent data corruption) sin intervención del administrador. • Protocolo nativo que impida la exposición directa de los datos almacenados ante ataques de ransomware, mediante intercepción pre-evento, y recuperación desde snapshot seguro inmutable. • Auditoría completa de versiones y eventos de acceso al sistema de archivos con retención configurable de registros, compatible con estándares de auditoría empresarial. • Soporte de integración con servicios de directorio compatibles con estándar LDAP v3, incluyendo Microsoft Active Directory y directorios compatibles LDAP de terceros. • Cifrado de datos en reposo y en tránsito mediante AES-256, con soporte para TLS 1.2 o superior e IPSec, y cumplimiento del estándar FIPS 140-2 o superior a nivel de hardware. • Soporte para listas blancas y listas negras de direcciones IP para restringir accesos no autorizados a los recursos del sistema. • Funcionalidad de recuperación rápida (Instant Recovery) para restaurar datos críticos en caso de ataque o falla, sin necesidad de restauración completa del volumen. • Verificación multi-administrador (Multi-Admin Verification) que garantice que acciones críticas como modificaciones de configuración, eliminación de datos o ajustes de seguridad requieran la validación y aprobación de más de un administrador, configurable según las políticas de seguridad de la entidad. • Capacidad para establecer reglas de acceso de forma individual por cada recurso o grupo de recursos, admitiendo la configuración de reglas entrantes y salientes entre el usuario y los recursos, garantizando que solo se acceda a los recursos autorizados y que los no autorizados permanezcan inaccesibles. Todas las funcionalidades de seguridad listadas deberán estar completamente licenciadas a perpetuidad en ambos sistemas, sin costos adicionales para la Policía Nacional. • El fabricante de los sistemas de almacenamiento ofertados deberá contar con certificación vigente bajo la norma ISO 14001:2015 Sistema de Gestión Ambiental o su equivalente, expedida por un organismo de certificación acreditado ante ONAC o entidad equivalente reconocida internacionalmente (DAkkS, UKAS, ANAB u otras). Esta certificación deberá estar vigente a la fecha de cierre del proceso y aplicar al proceso de fabricación de equipos de almacenamiento.		
GESTIÓN Y ADMINISTRACIÓN				
1.51.	Consola de administración centralizada	Cada sistema de almacenamiento deberá ser administrable desde una única interfaz de gestión centralizada vía web y CLI, completamente licenciada a perpetuidad para todos los atributos, características y funcionalidades. La consola deberá incluir como mínimo: manejo de alertas, gestión y presentación de filesystems, hosts e inventario de discos; snapshots y clones; dashboard en tiempo real con métricas de rendimiento y capacidad; generación de reportes automatizados sobre uso de almacenamiento, actividad y estado del sistema; y reporte de consumo de almacenamiento por pool y host. El acceso a la consola deberá asegurarse mediante SSL y HTTPS.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
		En caso de requerirse un servidor dedicado para la administración, este deberá ser entregado en alta disponibilidad (mínimo dos nodos en clúster), sin costo adicional para la entidad, con las siguientes características mínimas por nodo: • Factor de forma tipo rack máx. 1U • Procesador Intel Xeon Scalable de última generación lanzada en 2025 con mínimo 16 núcleos • 128 GB de memoria RAM • 2 x 1 TB NVMe SSD en RAID 1 • 2 puertos 25 GbE con módulos SFP28 • 2 puertos 32 Gb FC. • 1 puerto 1 GbE para gestión remota. • Fuentes de poder y ventiladores redundantes. • Sistema operativo licenciado a nombre de la Policía Nacional. • Todos los componentes de harware deben estar en alta disponibilidad.		
1.52.	Respaldo y Licenciamiento Veeam Backup & Replication	Conforme a la arquitectura tecnológica de cada fabricante, se requiere que la solución de almacenamiento ofertada permita la integración con Veeam Backup & Replication, software con el que actualmente cuenta la Policía Nacional de Colombia, garantizando la continuidad operativa y la protección de la información crítica. Para fortalecer la seguridad y disponibilidad de los datos de misión crítica, según las directrices del supervisor del contrato, se deberán suministrar 60 instancias de Veeam Data Platform Advanced con licenciamiento perpetuo (Legacy Perpetual Licensing), asegurando: • Soporte directo del fabricante 7x24 por un período mínimo de 3 años para las instancias de Veeam Data Platform Advanced. • Bolsa de 60 horas de soporte 8*5, para ser ejecutadas en un tiempo hasta de (3 años) a partir de la compra e instalación en la consola de Veeam Backup de la Policía Nacional a la cuenta licenciamiento@correo.policia.gov.co • Registro del licenciamiento a nombre de la Policía Nacional de Colombia a la cuenta licenciamiento@correo.policia.gov.co. • Los servicios de actualización e integración y pruebas del software de backup deberá ser realizados por el contratista a través de personal de veeam certificado en VMCE. Durante la vigencia de la garantía del contrato, el contratista deberá realizar de manera obligatoria las actualizaciones por ingenieros certificados en VMCE versión 12 o superior del software Veeam Backup & Replication cada vez que el fabricante libere una nueva versión oficial, así como ejecutar las pruebas necesarias que permitan verificar el correcto funcionamiento del ecosistema de respaldo, incluyendo sus componentes asociados, garantizando que dichas actividades se efectúen sin generar ningún costo adicional para la entidad contratante.		
1.53.	Software de gestión y replicación	Cada sistema de almacenamiento debe proporcionar gestión de recuperación ante desastres (DR) basada en interfaz gráfica de usuario (GUI) con un solo clic para aplicaciones. El sistema de gestión basado en GUI puede identificar automáticamente los recursos de las aplicaciones y admite protección, recuperación, conmutación por error y pruebas de DR, así como la gestión visualizada de DR. Admite la gestión unificada de DR para múltiples redes de DR, como protección local y DR activo-pasivo.		
1.54.	Gestión O&M inteligente con predicción proactiva	Cada sistema de gestión debe incluir capacidades de inteligencia artificial para predicción proactiva: fallas de disco con mínimo 14 días de anticipación, cuellos de botella de rendimiento con al menos 60 días de anticipación, y tendencias de capacidad con horizonte de 365 días.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ				
ITEM	**DESCRIPCION**		**CUMPLE**	**NO CUMPLE**
1.55.	Funcionalidades licenciadas (Value-Added Features)	Todas las funcionalidades de ambos sistemas (snapshots, clones, replicación síncrona/asíncrona entre los dos sistemas, deduplicación, compresión, thin provisioning, reportes, replicación, identificación contra ransomware, inmutabilidad.) deben estar licenciadas a perpetuidad y registradas a nombre de la Policía Nacional, sin costos adicionales.		
SOPORTE, GARANTÍA Y CICLO DE VIDA				
1.56.	Actualizaciones no disruptivas	Cada sistema debe permitir actualizaciones de OS y firmware sin interrupción del servicio.		
1.57.	Garantía de actualización sin migración por 5 años	El fabricante debe garantizar que el sistema entregado permita actualizaciones de hardware y software por un período mínimo de 5 (cinco) años desde la fecha de entrega, sin necesidad de migración de datos. Esto incluye actualización de controladoras, módulos I/O y firmware de forma no disruptiva, sin requerir reemplazos completos del sistema.		
1.58.	Fecha de garantía	Todo el hardware que hace parte del presente proceso debe tener un tiempo de garantía y soporte mínimo de cinco (5) años ofrecida por el fabricante, contados a partir de la fecha del acta de recibo a satisfacción por parte del Supervisor del contrato.		
CONFIGURACIÓN DE REPLICACIÓN ACTIVO-ACTIVO NAS Y OBJETOS S3 ENTRE SITIOS				
1.59.	Configuración de filesystem NAS	El contratista deberá configurar, probar y documentar el montaje del servicio de almacenamiento NAS de los sistemas adquiridos en todos los servidores de capa de aplicación con sistema operativo Oracle Linux 8 o superiores y en todos los servidores de base de datos del SECAD, utilizando el protocolo de acceso NAS compatible con cada sistema operativo intervenido. El alcance mínimo es el siguiente: • Configuración de exports NAS (en caso de ser necesario): El contratista deberá configurar en cada sistema de almacenamiento los exports necesarios, organizados por aplicación definiendo para cada export las IPs de los servidores autorizados, los permisos de acceso (lectura/escritura o solo lectura según corresponda), las opciones de seguridad y los parámetros de rendimiento mínimos (rsize/wsize de 1 MB). La estructura de directorios y la nomenclatura de los exports deberán ser propuestas por el contratista y aprobadas por el supervisor del contrato antes de su implementación. • Montaje en servidores de aplicación (Oracle Linux 8 / x86): El contratista deberá configurar el montaje persistente del servicio NAS utilizando el protocolo de acceso NAS compatible con Oracle Linux 7/8/9, registrándolo en /etc/fstab de cada servidor de capa de aplicación de forma que el montaje se restaure automáticamente tras reinicios del servidor. • Seguridad del acceso NAS: Los exports deberán restringirse exclusivamente a las IPs de los servidores autorizados, sin permitir exports abiertos a rangos de red completos. Deberán configurarse con la opción root_squash para que el usuario root de los servidores cliente no tenga privilegios de root sobre el NAS. • Documentación técnica: El contratista deberá entregar la documentación completa que incluya: topología del servicio NAS y su integración con los servidores, configuración de exports del almacenamiento, configuración de montajes en cada servidor intervenido, matriz de acceso por servidor y export, resultados de las pruebas de rendimiento y disponibilidad, y el procedimiento operativo para agregar nuevos servidores al servicio NAS en el futuro.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
2.	**GENERALIDADES**		
2.1.	El contratista deberá suministrar e instalar el kit de rieles, cables de gestión, así como todos los componentes y accesorios necesarios para garantizar el correcto funcionamiento e integración de la solución ofertada. Estos elementos deben ser compatibles con el sistema y cumplir con los estándares de calidad y desempeño establecidos por el fabricante, asegurando una instalación eficiente, segura y operativa.		
2.2.	El contratista, en colaboración con el fabricante, deberá elaborar y presentar un cronograma detallado con las actividades específicas que se llevarán a cabo para la implementación de la solución de los sistemas de almacenamiento. Este cronograma deberá ser entregado al supervisor de contrato para su aprobación dentro de los primeros 15 días calendario a partir de la aprobación de la garantía única. El cronograma debe contemplar todas las fases del proyecto, incluyendo planificación, instalación, configuración, pruebas y puesta en marcha, asegurando que todas las actividades se realicen de acuerdo con los plazos establecidos y sin comprometer la operación del sistema. Los alcances del proceso deben ser gestionados bajo principios de confidencialidad, integridad, disponibilidad y criticidad de la información, garantizando la implementación y migración de los sistemas no afecte la seguridad ni la operatividad de los datos almacenados.		
2.3.	El contratista deberá contar con un conocimiento detallado de la **topología de conexión y disponibilidad de la infraestructura** en los centros de datos **principal** y **alterno** de la Policía Nacional. En caso de que los equipos ofertados superen las capacidades técnicas disponibles en la infraestructura del centro de datos (principal), el contratista será responsable de proporcionar y garantizar la instalación de los componentes adicionales de electricidad y conectividad de datos necesarios para el correcto funcionamiento de los sistemas de almacenamiento y sus servicios. Para asegurar la homogeneidad y compatibilidad con la infraestructura actual, todo el cableado de cobre y/o fibra óptica deberá ser de la misma marca y modelo que el fabricante actual del centro de datos. Además, estos elementos deben estar certificados en sus puntos de enlace LAN o SAN para poder tramitar la garantía de 25 años proporcionada por el fabricante. **Integración de cableado** El contratista deberá garantizar el suministro de cableado certificado SIEMON en la instalación del almacenamiento, dado que la Policía cuenta con todo el cableado del DataCenter certificado, el cableado y los puntos deberán quedar certificados por SIEMON, estos certificados deberán anexarse en la documentación que se entregue al finalizar el contrato y validado por el supervisor del contrato. **Normas de Organización y Certificación del Cableado** Para garantizar la adecuada organización de la infraestructura de almacenamiento, el contratista deberá proporcionar un servicio especializado que certifique: Todo el cableado estructurado debe contar con servicio especializado suministrado por el contratista donde certifique el peinado de los Rack de datos, asegurando el cumplimiento de normas de marquillado y organización de cableado de datos y de servidores.		
2.4.	El contratista debe suministrar y configurar para los equipos los siguientes componentes de cableado estructurado: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 3 Meter, Marca Siemon, parte No. FBP-LCLC5V-03AH o 19SIFBPLCLC5V03AH, cantidad para todos los puertos de tarjetas LAN de los equipos. SFP+ AFBR-709SMZ-IB8 10GBASE-SR cantidad 110.10.6. Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Erika Violet, LSOH-3C, 3 Meter, Marca Siemon, parte No. FBP-LCLC5V-03EH o 19SIFBPLCLC5V03EH, Cantidad para todos los puertos de tarjetas SAN de los equipos.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	Copper, Patch Cord, RJ45, RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack, longitud requerida en sitio, marca Siemon, parte No. ZM6A-S07-06B o 19SIZM6AS0706B, Cantidad para todos los puertos de tarjetas de GESTIÓN de los equipos.		
2.5.	El almacenamiento y equipamiento adicional ofertados deberán poderse comunicar a través de los protocolos SNMP V3 y proveer los archivos MIB'S que permitan la lectura de los diferentes parámetros de monitoreo de cada uno de uno de los equipos, el contratista deberá garantizar que el almacenamiento deberá ser integrado en la herramienta a través de SNMP que ofrece el almacenamiento requerido en el presente proceso.		
2.6.	Los servidores y sistema de almacenamiento junto con el equipamiento adicional suministrado en este proceso deberán contar con una rotulación individualizada y estandarizada, garantizando una identificación clara, precisa y conforme a los lineamientos técnicos y operativos establecidos por la supervisión del contrato. La identificación de cada equipo y conexión deberá cumplir con los siguientes criterios: • Identificación única y funcional: Cada dispositivo de almacenamiento y sus conexiones deberán contar con una etiqueta que refleje su funcionalidad dentro del sistema, su ubicación y su asignación específica dentro de la infraestructura. • Cumplimiento de normativas institucionales: La rotulación deberá alinearse con los estándares de la Policía Nacional en cuanto a identificación de equipos tecnológicos, seguridad y trazabilidad. • Material resistente y duradero: Se utilizarán etiquetas de alta durabilidad, resistentes a factores ambientales como temperatura, humedad y manipulación frecuente, asegurando su legibilidad durante toda la vida útil del equipo. Codificación y trazabilidad: Los rótulos deberán incorporar un sistema de codificación estructurado, permitiendo la fácil identificación, rastreo y gestión de cada componente a lo largo de su ciclo de vida, facilitando los procesos de mantenimiento, monitoreo y actualización.		
2.7.	El contratista deberá llevar a cabo todas las actividades y tareas preliminares necesarias para la correcta ejecución del presente proceso, garantizando el cumplimiento de los requisitos técnicos, operativos y de seguridad establecidos. Estas actividades incluyen, pero no se limitan a: • Inspección y diagnóstico inicial: Evaluación de las condiciones del sitio, infraestructura existente y posibles restricciones técnicas. • Planificación y coordinación: Elaboración de un plan de trabajo detallado, incluyendo cronograma de ejecución y asignación de recursos. • Gestión de permisos y autorizaciones: Trámite de accesos, permisos de trabajo y demás requisitos administrativos necesarios. • Adecuaciones previas: Preparación del área de trabajo, incluyendo desmontaje, limpieza y adecuaciones necesarias para la instalación de los equipos y componentes. Verificación de suministros y compatibilidad: Revisión de los materiales, herramientas y equipos a utilizar, asegurando su compatibilidad con la infraestructura existente.		
2.8.	El contratista será el responsable de entregar en correcto funcionamiento todos los bienes y servicios para la ejecución del presente proceso de contratación, para ello, dentro de su oferta económica debe incluir el costo de todas las actividades requeridas para ese fin. Cualquier actividad adicional, así como cualquier labor de planeación, programación, desarrollo, tiempos de disponibilidad de personal, suministro de equipos, componentes de conectividad y software, que se requieran para garantizar el pleno y adecuado funcionamiento de los equipos de almacenamiento, deben ser incluidos por el contratista y por ningún motivo generarán costos adicionales a la Policía Nacional.		
2.9.	El contratista en coordinación con el fabricante, presentarán la arquitectura y planes de trabajo para la implementación de los equipos ofertados, migración de los datos del antiguo almacenamiento, entre otras actividades necesarias para el cumplimiento de los requerimientos técnicos. La arquitectura debe cumplir con las buenas prácticas de implementación recomendadas por el fabricante del almacenamiento ofertado, en los casos en que los equipos evidencien cuellos de botella o afectaciones causadas por configuraciones o falta de componentes, el contratista deberá suministrar sin costo adicional para la Policía Nacional, los componentes y/o equipamientos y/o actividades de		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	servicio profesional que sean necesarios para garantizar la operación normal de los equipos en la plataforma de misión crítica de la Policía Nacional.		
2.10.	El contratista deberá garantizar la disponibilidad del personal de profesionales durante la ejecución del contrato para la realización de las tareas y actividades requeridas en la implementación de los almacenamientos.		
2.11.	El contratista incluirá sin costos para la Policía Nacional todos los servicios necesarios para la instalación, configuración, balanceo, migración de datos y puesta en funcionamiento de todo el hardware y software objeto del presente proceso.		
2.12.	Los servicios de instalación, configuración, balanceo, deberá ser suministrados directamente por el fabricante. La migración de datos, puesta en funcionamiento y transferencia de conocimientos deberán ser suministrados directamente por el contratista con apoyo del fabricante.		
2.13.	El contratista garantizará que la instalación, configuración y pruebas serán realizadas con personal certificado por el fabricante y entregará en completa operación llave en mano todos los elementos necesarios como, interfaz de conexión como patch-cord termoformados de fábrica, cables FC, transceivers de fibra óptica en origen y destino, software de configuración (drivers) y utilitarios del sistema para cada uno de los componentes de la solución que garanticen su pleno funcionamiento.		
2.14.	El almacenamiento ofertado debe tener la capacidad de ser actualizados en todos sus componentes (firmware) sin causar afectación del servicio.		
3.	**SOLUCIÓN DE COBRE CABLE UTP EN CATEGORÍA 6A (Si se requiere)**		
3.1.	Debe cumplir o superar las especificaciones de la norma ANSI/TIA-568-2-D, el estándar IEEE 8010.10.2.3an-2006 de requerimientos de canal para soportar 10GBASE-T.		
3.2.	Debe soportar por lo menos las siguientes aplicaciones: 100 Mb/s Ethernet 10GBase-T, 100Base-TX (Fast Ethernet), 1000base-T (Gigabit Ethernet); IEEE 8010.10.2.3, ANSI X10.10.3.263; 1.2Gb/s ATM; Token Ring 4/16 para Voz y Datos.		
3.3.	Debe existir compatibilidad mecánica y eléctrica de los productos y cables de la Categoría 6A, con las categorías anteriores.		
3.4.	El recubrimiento debe ser continuo, sin porosidades u otras imperfecciones, con especificación de su cubierta o chaqueta type LSZH (UL o ETL) de acuerdo a la norma IEC 60332-10.10.3. Retardante de llama, no generar gas tóxico y libre de halógenos (LSZH).		
3.5.	El cable debe ser de construcción tubular en su apariencia externa (redondo). Dentro del cable, los conductores de cobre deben estar trenzados en pares firmemente y éstos deben tener separación individual para mejorar su desempeño. El cable deberá ser calibre No. 23 AWG, Debe ser elaborado por el mismo fabricante de la conectividad y estar probados por laboratorio ETL para Categoría 6A respectivamente.		
3.6.	Los enlaces con cables de cobre deben ser de 4 pares trenzados sólidos, del tipo F/UTP (blindado). La conexión final a los patch panels correspondientes se deberá hacer con el método de conexión T568B.		
3.7.	No se aceptarán cables con conductores pegados u otros métodos de ensamblaje que requieran herramientas especiales para su terminación.		
3.8.	Debe poseer un elemento que ayude a reducir los efectos de alíen Cross Talk		
3.9.	El recubrimiento del cable debe ser color azul y tener impresa, como mínimo, la siguiente información: nombre del fabricante, número de parte, tipo de cable, número de pares, tipo de listado (LSZH), y las marcas de mediciones secuenciales para verificación visual de longitudes.		
3.10.	El cable debe permitir en su instalación al menos un radio mínimo de curvatura de 4 veces su diámetro externo a una temperatura de 0º C sin ocasionar deterioro en forro o aislantes.		
3.11.	Velocidad de propagación >69% de 10 a 500 Mhz, Debe poseer una impedancia característica de 100Ω, +/- 15% hasta 100Mhz, +/- 22% entre 100 – 350Mhz y +/- 32% entre 350 – 500Mhz de respuesta para ancho de banda de acuerdo con el ANSI/TIA 568-2-D para categoría 6 A.		
3.12.	Debe cumplir con IEEE 8010.10.2.3af, IEEE 8010.10.2.3at y los requerimientos de 8010.10.2.3bt		
3.13.	La clasificación de flamabilidad de la chaqueta debe cumplir con IEC 60332-3, 60754-2, 61034-2		
3.14.	Para la instalación de los enlaces de cobre en los EDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels ZMAX, Empty, Shielded, 48 Openings, Angled, 1U, Black, Fixed Wire Manager, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional		
3.15.	Para la instalación de los enlaces de cobre en los HDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels inteligentes del tipo MapIT, Empty, Shielded, 24 Openings,		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	Angle, 1U, Black, Fixed Wire Manager, Keystone, Referencia Siemon: M-SPPA-K24ENS, los cuales deberán estar conectados a un panel de control maestro MapIT, 24 Port, 1U, Black, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional. Es importante que el proveedor verifique si existe disponibilidad de puertos de conexión en el panel de control maestro, en caso de que no haya disponibilidad será necesario instalar un panel de control maestro adicional.		
3.16.	Para los herrajes de patch panel del sistema inteligente ubicados en los HDA´s los cables de cobre deberán ser instalados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Keystone, Black, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
3.17.	Para los herrajes de patch panel ubicados en los EDA´s los cables de cobre deberán ser terminados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Panel Mount, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
3.18.	Para la habilitación de los servicios en los EDA´s será necesario utilizar patch cords RJ45 a RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack. Para la habilitación de los servicios en los HDA´s será necesario utilizar patch cords del sistema inteligente MapIT, RJ45 a RJ45, Category 6A, U/FTP, T568A/B, Stranded, LSOH-1, Blue Cable, Blue Boot, 2 Meters, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
3.19.	Todos los componentes de cobre (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con un equipo de certificación avalado por el fabricante del cableado de cobre, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas se deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
3.20.	Para la conexión de COBRE ADMINISTRACIÓN se requiere que el contratista instale: Copper, Patch Cord, RJ45, RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack 3 Meter, No. parte ZM6A-S07-06B 19SIZM6AS0706B, Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico ofertado		
4.	**SOLUCIÓN DE FIBRA ÓPTICA (Si se requiere)**		
4.1.	Los enlaces con cables de fibra óptica pre-conectorizados deberán ser MTP/MPO de 12 hilos, del tipo multimodo OM4, y velocidades de hasta 10 Gbseg hasta 550 metros sobre enlaces dúplex (2 hilos) o velocidades de hasta 40 Gbseg sobre 4 enlaces dúplex (8 hilos).		
4.2.	Estos cables de fibra deben ser Plug & Play, Trunk, 12 Strand, RazorCore, XGLO, Multimode, Female MTP Base 12 Solution, Female MTP Base 12 Solution, Polarity C, OM4, 50/125, Aqua, LSOH-3C, Pulling Eye, XX Meter, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional (XX corresponde a la distancia en metros).		
4.3.	Para la conexión de los enlaces de fibra óptica en los HDA´s 3 (Bandeja de alta densidad) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo LightStack, Rack Mount, 1U, Sliding Access, 12 Openings, Black, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.4.	Para la conexión de los enlaces de fibra óptica en los EDA´s (Bandeja de conexión) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC, MTP, OM4, Black, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.5.	Como el sistema de fibra óptica es inteligente y está característica se realiza en los gabinetes EDA's bajo una topología de cross conexión se deben utilizar también bandejas u ODF´s (Bandeja de Cross conexión) de fibra óptica del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC a LC, OM4, Black, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.6.	Para la adecuada conexión de los cables de fibra óptica MTP/MTP a las bandejas de fibra óptica u ODF´s (Cassettes pre conectorizados) es requerido que estos cables sean conectados a cassettes pre conectorizados del tipo MTP a 6 LC dúplex, OM4, multimodo, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.7.	Para la conexión de equipos en los EDA´s y HDA´s se deberán utilizar patch cords entre las bandejas inteligentes de cross conexión de los EDA´s a los puertos de los equipos y las bandejas de alta		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	densidad a los puertos de los switches de fibra en los HDA´s, estos patch cords deberán ser dúplex, XGLO, Multimode, LC BladePatch a LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 2 Meter, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.8.	Adicionalmente, como la topología de conexión en los EDA´s es de cross conexión y el sistema es inteligente, es requerido utilizar patch cords dúplex del tipo inteligentes entre la bandeja que recibe los cables troncales de fibra MTP/MPO en cassettes pre conectorizados y la bandeja de cross conexión que habilita los servicios de los equipos, estos patch cords deben ser del tipo MapIT, Duplex, XGLO, Multimode, LC a LC, OM4, 50/125, Aqua, OFNR, 1 Meter, de la misma marca del fabricante instalado en el Centro de Datos de la Policía Nacional.		
4.9.	En caso de instalar enlaces nuevos de fibra óptica el contratista deberá verificar si hay disponibilidad de espacio en las bandejas de alta densidad de los HDA´s, en las bandejas inteligentes de los EDA´s, y en las bandejas inteligentes de cross conexión de los EDA´s, en caso de no tener disponibilidad deberán entregar e instalar bandejas nuevas con las especificaciones técnicas anteriormente descritas.		
4.10.	Todos los componentes de fibra óptica (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con un equipo de certificación avalado por el fabricante del cableado, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas se deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
4.11.	Para la conexión de FIBRA SAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Erika Violet, LSOH-3C, 5 Meter. No. Parte FBP-LCLC5V-05EH o 19SIFBPLCLC5V05EH, Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico ofertado		
4.12.	Para la conexión de FIBRA LAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 5 Meter. No. parte FBP-LCLC5V-05AH 19SIFBPLCLC5V05AH. Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico ofertado		
4.13.	Los enlaces con cables de fibra óptica pre-conectorizados deberán ser MTP/MTP de 12 hilos, del tipo multimodo OM4, y velocidades de hasta 10 Gbseg hasta 550 metros sobre enlaces dúplex (2 hilos) o velocidades de hasta 40 Gbseg sobre 4 enlaces dúplex (8 hilos).		
5.	**GARANTÍA**		
5.1.	El contratista deberá entregar una póliza de garantía integral que cubra tanto las refacciones como la calidad de los componentes suministrados. Esta garantía debe asegurar el buen funcionamiento de todo el equipamiento durante el período establecido, incluyendo la cobertura de cualquier defecto de fabricación o mal funcionamiento relacionado con los componentes del sistema de almacenamiento. La póliza deberá especificar claramente los términos de cobertura, los plazos de garantía, así como los procedimientos para la atención y resolución de incidencias, garantizando la reposición o reparación de los elementos defectuosos sin costo adicional para la Policía Nacional		
5.2.	Todo el hardware involucrado en el presente proceso deberá contar con una garantía proactiva y reactiva ofrecida directamente por los fabricantes, con una cobertura mínima de cinco (5) años. La garantía proactiva incluirá actualizaciones de firmware de manera semestral (dos veces al año), o cada vez que el fabricante libere una nueva versión de actualización, así como la actualización de software anual. La garantía reactiva cubrirá el mantenimiento correctivo 24/7 con un tiempo de respuesta de cuatro (4) horas, garantizando la reparación o reemplazo de equipos defectuosos en el menor tiempo posible. El contratista deberá proporcionar una carta dirigida a la Policía Nacional, firmada por los fabricantes de hardware que certifique la cobertura de las garantías directas de cada componente por un período no inferior a cinco (5) años. Esta certificación deberá incluir los números de serie de los equipos, los identificadores de licencias del software y/o los números de parte, especificando claramente que dichos componentes están cubiertos por el programa de mantenimiento preventivo en horario de 5x8 (con actualizaciones de versión dos veces al año o cada vez que el fabricante libere y estabilice una nueva versión) y mantenimiento correctivo en horario 7x24, con la obligación de contar con personal técnico en sitio para atender cualquier requerimiento relacionado.		
5.3.	El tiempo de garantía para cada ítem ofertado comenzará a partir de la fecha de firma del acta de recibo a satisfacción de los elementos por parte del supervisor del contrato. Esta garantía cubrirá todos los aspectos técnicos y operativos de los equipos y componentes suministrados, y se aplicará		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	exclusivamente a partir de la validación y aceptación formal de los mismos, según los términos establecidos en el proceso de entrega y puesta en marcha.		
5.4.	Horario de atención de 7x24x365, para la atención de casos proactivos y reactivos durante el periodo de garantía.		
5.5.	La solución debe incluir garantía calidad del servicio y correcto funcionamiento por cinco (5) años para el almacenamiento y servidores y, 2 años para el software de backup, la garantía de calidad de los bienes incluye partes, actualización de firmware y accesorios.		
5.6.	El tiempo de garantía para cada ítem ofertado inicia a partir de la fecha del acta de recibo a satisfacción de los elementos por parte del supervisor del contrato.		
5.7.	Durante el periodo de garantía, el proveedor deberá suministrar todos los repuestos (*nuevos, no remanufacturados*) de iguales o superiores características a los originales, sin costo alguno para la Policía Nacional para el almacenamiento. Para el caso del software, el proveedor deberá instalar las actualizaciones de firmware y versiones que sean lanzadas en el mercado durante la vigencia de la garantía sin costo para la Policía Nacional, con el fin de garantizar el correcto funcionamiento del equipo, por tal motivo deberá entregar bolsa de horas proactivas por cada año para actualizar los almacenamientos.		
5.8.	El contratista debe garantizar que el soporte técnico se preste a través de la garantía del fabricante.		
5.9.	Cuando se presenten fallas generales o particulares en los equipos, el fabricante debe dar soporte en sitio con personal certificado y experimentado en un tiempo máximo de cuatro (4) horas, contadas a partir de la fecha y hora de haber realizado el reporte del caso en la mesa de servicio.		
5.10.	Durante el periodo de garantía, el proveedor se compromete a reparar el equipo y dejarlo en perfecto estado de funcionamiento en un tiempo máximo de cuarenta y ocho (48) horas contadas a partir de la fecha y hora de haber realizado el reporte de la falla.		
5.11.	En caso de que la reparación del equipo demore más de cuarenta y ocho (48) horas, el proveedor deberá suministrar en forma inmediata un equipo de soporte de iguales o superiores características durante el tiempo que dure la reparación.		
6.	**SOPORTE Y MANTENIMIENTO**		
6.1.	El contratista deberá garantizar la disponibilidad permanente de canales de comunicación eficientes y accesibles para el reporte, gestión y seguimiento de incidencias relacionadas con el sistema de almacenamiento de datos no estructurados. Para ello, deberá proporcionar y mantener operativos, durante la vigencia del contrato, los siguientes medios de atención: **Plataforma de mesa de servicio o autoservicio web:** • Acceso vía web con interfaz intuitiva y segura. • Capacidad para generar, visualizar y hacer seguimiento de reportes o ticket • Registro detallado de cada ticket con trazabilidad y tiempos de respuesta. **Línea telefónica de soporte:** • Atención disponible y habla hispana en el horario acordado con la supervisión del contrato. • Personal técnico capacitado para recibir, clasificar y escalar incidencias. **Correo electrónico dedicado para soporte:** • Cuenta exclusiva para la recepción y gestión de solicitudes. • Confirmación automática de recepción de casos con número de ticket asignado. Todos estos medios deberán cumplir con los estándares de seguridad, disponibilidad y accesibilidad definidos por la Policía Nacional, asegurando una gestión eficiente y oportuna de los incidentes o de información de carácter general relacionado con el componente tecnológico entregado a la Entidad.		
6.2.	El contratista debe garantizar soporte técnico en español, disponible de manera remota a través de canales telefónicos e Internet, como primer nivel de atención. Este soporte debe ser accesible durante el horario establecido para la atención de incidencias 7x24 y deberá contar con personal capacitado para resolver problemas técnicos de forma eficiente y efectiva, asegurando una respuesta oportuna y la continuidad operativa.		
6.3.	El grupo de soporte del contratista debe garantizar que el ticket del problema tenga un seguimiento adecuado, oportuno, se maneje de forma rápida y eficientemente, y se lleve a los niveles adecuados hasta su cierre. Además, se debe tener informado constantemente por escrito, los progresos al		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	supervisor del contrato y al Técnico de infraestructura del Centro de Procesamiento de Datos de la Policía Nacional.		
6.4.	Al inicio del contrato se establecerá el procedimiento de solicitud de la garantía y soporte técnico tanto para el hardware como para el software ofertados.		
6.5.	Durante el tiempo de la garantía se debe prestar todo el acompañamiento necesario para realizar las actualizaciones de la solución, cuando se instalen nuevas versiones.		
6.6.	Establecer y brindar planes de mantenimiento preventivo y correctivo durante la garantía para toda la solución ofertada.		
6.7.	El contratista debe recomendar procedimientos operacionales que mitiguen los riesgos de fallas del sistema.		
6.8.	A partir de la entrega y recepción a satisfacción de la solución, el contratista deberá proporcionar un período mínimo de tres (3) meses de acompañamiento y consultoría técnica para garantizar la estabilidad, optimización y mejora continua de la plataforma. Durante este período, el contratista deberá: • Brindar soporte especializado ante cualquier incidente, falla o ajuste necesario para optimizar el desempeño de la solución. • Realizar ajustes y afinamiento en la configuración del sistema, asegurando su correcta operación y alineación con los requerimientos de la Policía Nacional. • Generar recomendaciones de mejora basadas en el monitoreo del desempeño y las necesidades operativas. • Capacitar al personal designado, si es necesario, en el uso y administración eficiente de la solución implementada. Este acompañamiento deberá garantizar la continuidad operativa y la estabilidad de la plataforma, minimizando riesgos y asegurando el cumplimiento de los objetivos del proyecto.		
7.	**ENTREGA SOLUCIONES**		
7.1.	La aceptación final de la adquisición del sistema de almacenamiento de información no estructurada se realizará una vez el contratista haya entregado e implementado todos los componentes de hardware y software con sus versiones actualizadas, garantizando compatibilidad, seguridad y estabilidad. Se deberá completar la migración de datos, el balanceo de carga, asegurando la integridad y disponibilidad de la información. Además, se validará la integración con los sistemas de gestión, la interoperabilidad y el cumplimiento de protocolos de seguridad. La funcionalidad del sistema será monitoreada durante 10 días posteriores a la puesta en marcha, asegurando su correcto desempeño en condiciones normales de operación. Finalmente, la aceptación se formalizará mediante la firma de actas de verificación y cumplimiento de requisitos técnicos y operativo.		
7.2.	El Contratista debe entregar para el recibo a satisfacción de las plataformas los siguientes documentos: Documentación de la arquitectura de la solución donde se detallen componentes físicos, lógicos, conectividad y fuentes de información. Certificado del fabricante de la capacidad en PB (Petabytes) RAW y usables suministrada en cada solución de almacenamiento.		
7.3.	Los servicios de instalación, configuración, balanceo, transferencia de conocimientos y puesta en funcionamiento deben ser suministrados directamente por el fabricante con ingenieros certificados en el software y hardware ofertado.		
7.4.	Todos los componentes de los almacenamientos deben ser instalados en los racks o gabinetes que se encuentran disponibles en el centro de datos principal y alterno de la Policía Nacional que cuentan con las siguientes características: estándar de 42U (profundidad 120Cm y ancho de 60cm) y PDU Gabinetes 30Amp de 30-(C13) y 6-(C19) PDU (100 - 240 VAC). Los sistemas de almacenamiento deberán ser integrados y configurados en la solución GRAFANA Y ZABBIX del Centro de Procesamiento de Datos, por lo cual el almacenamiento deberá ser compatible con el protocolo SNMP para su monitoreo		
7.5.	Las actividades de migración deberán garantizar la seguridad, integridad, consistencia y no disrupción de los servicios que actualmente se encuentran configurados en el Centro de Procesamiento de Datos de la Policía Nacional.		
7.6.	El contratista deberá ejecutar en conjunto con el fabricante, la activación e implementación de las licencias de replicación para futuras adquisiciones de almacenamiento.		
7.7.	El contratista en coordinación con el fabricante, deberá entregar todas las conexiones SAS o NMVe de mejor rendimiento disponible en el mercado, igualmente, deberá realizar actividades de implementación en las cuales la totalidad de conexiones queden equilibradas en los gabinetes de		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	discos y controladoras, estas configuraciones deberán ser certificadas por el fabricante describiendo el cumplimento de las buenas prácticas recomendadas para los modelos ofertados.		
7.8.	Los gabinetes de discos que no cuenten con discos, deberán ser entregados con unidades de relleno para conservar el flujo de aire en los equipos. Así mismo, deberán ser suministrados la totalidad de módulos de entrada y salida, fuentes de alimentación eléctrica y enfriamiento que soporte el equipo.		
7.9.	Los almacenamientos ofrecidos deberán ser configurados sin punto único de falla, incluyendo controladoras, tarjetas de memoria caché, ventiladores, fuentes de poder, conexiones SAS entre otros.		
8.	**CERTIFICADOS**		
8.1.	Con el fin de garantizar la calidad del servicio y el cumplimiento en la ejecución del contrato, se requiere que el contratista adjunte carta expedida por el fabricante con representación en Colombia, en la que certifique que el contratista o su proveedor/aliado es distribuidor autorizado para suministrar los equipos definidos en el presente proceso para el almacenamiento En la certificación para el almacenamiento, se debe indicar el número del presente proceso, garantizando que la ejecución de los servicios será realizada directamente por el fabricante o contratista con representación en Colombia; especificando línea telefónica y email del fabricante. Si la certificación no se puede validar su procedencia y legitimidad no será tenida en cuenta.		
8.2.	El contratista deberá incluir en su propuesta una certificación expedida por el fabricante que garantice la ejecución de mantenimientos preventivos y proactivos al componente de hardware por un período mínimo de cinco (5) años realizado por el fabricante, asegurando la continuidad operativa y el óptimo desempeño de la solución.		
8.3.	El contratista deberá adjuntar a su propuesta una certificación que acredite que los equipos ofertados no se encuentran en la fase de fin de vida útil (End of Life - EOL), garantizando su disponibilidad, soporte y actualizaciones por parte del fabricante.		
8.4.	El contratista deberá incluir la documentación técnica oficial que demuestre la compatibilidad y homologación del almacenamiento ofertado con el software Veeam Backup & Replication. adicionalmente deberá suministrar certificación de partner autorizado o mínimo enrolled. Para ello, deberá cumplir con los siguientes requisitos: Se deberá anexar el certificado emitido directamente por Veeam Backup & Replication o el fabricante del almacenamiento propuesto, que acredite que el almacenamiento ofertado es compatible con el software de backup y ha sido probado para su compatibilidad y operación con este software de respaldo. Este requisito es fundamental para la entidad, dado que Veeam Backup & Replication es la solución actualmente implementada para la protección y resiliencia de los datos de la Policía Nacional. Dicho certificado deberá garantizar la total compatibilidad e integración del almacenamiento ofertado con la versión más reciente y estable de Veeam Backup & Replication, específicamente la versión 12.3, actualmente implementada en la institución. La solución deberá contar con soporte oficial del fabricante para cualquier requerimiento de integración con Veeam.		
8.5.	El contratista deberá presentar en su propuesta documentación oficial por el fabricante del almacenamiento en el cual certifique o avale sus mecanismos de protección contra ransomware.		
9.	**TRANSFERENCIA DE CONOCIMIENTO**		
9.1.	Capacitación para la administración y gestión de los servidores, de acuerdo con los requerimientos del presente pliego. Se designará los funcionarios correspondientes del grupo administración de servicios de infraestructura en la nube para las capacitaciones, a lo cual se debe tener en cuenta las siguientes consideraciones: • El contratista debe suministrar transferencia de conocimiento de la solución ofertada con los niveles de configuración, administración, soporte y gestión de los equipos, los cursos deben tener una intensidad de mínimo 40 horas, para mínimo ocho (8) funcionarios. • Los entrenamientos deben dictarse en centros de enseñanza autorizados por los fabricantes en la ciudad de Bogotá con una intensidad diaria no mayor a 4 horas, incluyendo todos los elementos y costos asociados al entrenamiento. Se debe entregar la respectiva certificación de asistencia para cada curso a los funcionarios participantes.		

ADQUISICIÓN DE INFRAESTRUCTURA CONVERGENTE (ALMACENAMIENTO SAN/NAS PARA LA POLICÍA METROPOLITANA DEL VALLE DE ABURRÁ			
ITEM	**DESCRIPCION**	**CUMPLE**	**NO CUMPLE**
	• Se deberá proporcionar una capacitación en Project Management Professional (PMP®) en idioma español, con una duración mínima de 40 horas, dirigida a tres (3) funcionarios. La capacitación debe estar alineada con los estándares del Project Management Institute (PMI) y cubrir los lineamientos del PMBOK® y demás guías aplicables. Se deberá incluir vouchers para la presentación del examen de certificación PMP®, garantizando dos (2) oportunidades de presentación para tres (3) funcionarios. Se deberá proporcionar acceso a un simulador de preguntas oficiales del PMI, con preguntas actualizadas y formuladas directamente por el instituto, permitiendo la preparación efectiva de los participantes para el examen.		