ANEXO TÉCNICO

OBJETO: REALIZAR LA RENOVACIÓN Y EXTENSIÓN DEL SOPORTE Y GARANTÍA DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DATA CENTER ALTERNO (DCA), ASÍ COMO EL SUMINISTRO E IMPLEMENTACIÓN DE LOS COMPONENTES REQUERIDOS PARA EL FORTALECIMIENTO DE LOS DATA CENTER DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO.



SECRETARÍA DE EDUCACIÓN DEL DISTRITO

BOGOTÁ – COLOMBIA

AGOSTO DE 2026

BOGOTÁ | SECRETARÍA DE EDUCACIÓN

TABLA DE CONTENIDO

1. DESCRIPCIÓN DE LA NECESIDAD 5
1.1. Renovación de soporte y garantía de la infraestructura tecnológica de Datacenter Alterno DCA 7
1.2. Fortalecimiento de la Infraestructura tecnológica de Datacenter Principal DCP 8
1.3. Fortalecimiento infraestructura de Datacenter NVC 9
1. OBJETO 10
2. ALCANCE DEL SERVICIO 10
3. CÓDIGOS UNSPSC 11
4. DESCRIPCIÓN DE LA RENOVACIÓN DE SOPORTE Y GARANTÍA 12
5. DESCRIPCIÓN DEL SUMINISTRO E IMPLEMENTACIÓN DE COMPONENTES PARA LOS DATA CENTER . 17
5.1. MÓDULOS INTEGRADOS TIPO MICRO CENTRO DE DATOS 17
5.1.1. Protección integral de la infraestructura hiperconvergente del DCP 17
5.2. SERVIDOR PARA DIRECTORIO ACTIVO Y DHCP EN NVC 18
5.2.1. Fortalecimiento de servicios de Directorio Activo y DHCP en NVC 18
6. LUGAR DE ENTREGA 19
7. PLAZO DE EJECUCIÓN DEL CONTRATO 20
8. FORMA DE PAGO 20
9. SERVICIOS DE SOPORTE 22
10. SERVICIOS DE RENOVACIÓN Y EXTENSIÓN DE GARANTÍA FABRICANTE PARA INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA DATA CENTER ALTERNO (TABLA 1.) 23
11. SERVICIOS DE GARANTÍA DE FABRICANTE PARA COMPONENTES DE DATA CENTERS DCP y NVC SUMINISTRADOS 23
12. GARANTÍAS 24
13. COMPONENTES OBJETO DE LA EXTENSIÓN DE GARANTÍA 25
13.1. Sistema Modular de Data Center 25
13.1.1. Especificaciones de soporte y garantía estándar integral para Sistema Modular Datacenter - FM2000 25
13.2. Infraestructura de Red – Core y Distribución 26
13.2.1. Especificaciones de Soporte y Garantía HI CARE para Switches Tor 27
13.3. ONT Red de Acceso Óptico - GPON 28
13.4. OLT Red de Acceso Óptico - GPON 28
13.5. Sistema de Detección (Edwards) y Extinción (SEVO Systems) de Incendios y Alarma (Kidde) 28
13.6. Sistema de Respaldo Eléctrico 30
13.6.1. Especificación del Servicio 30
13.6.2. Requisitos del Oferente 31

14. COMPONENTES DE FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DE DATACENTER PRINCIPAL DCP 31
14.1. Especificaciones técnicas módulos integrados tipo micro centro de datos 31
15. COMPONENTES FORTALECIMIENTO INFRAESTRUCTURA DE DATACENTER NVC 33
15.1. Especificaciones técnicas Servidor Datacenter NVC 33
16. PLAN DE MANTENIMIENTO PREVENTIVO PARA INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA DATA CENTER ALTERNO (TABLA 1.) 37
16.1. Guía de especificación de plan de mantenimiento 37
17. CERTIFICACIÓN DE LA CASA MATRIZ, AUTORIZACIÓN DE SERVICIOS 41
17.1. Certificación de fabricante requerida – Soporte Módulo inteligente FM2000 41
17.2. Certificación de fabricante requerida – Soporte Especializado Switches Huawei 42
17.3. Certificación de fabricante requerida – Soporte Planta Eléctrica 42
17.4. Certificación de fabricante requerida – Sistema de Detección de Incendios 43
17.5. Certificación de fabricante requerida – Sistema de Extinción de Incendios 44
17.6. Certificación de fabricante requerida – Sistemas Inteligentes de Alarma contra Incendios 44
17.7. Certificación de fabricante requerida – Módulo integrado tipo micro centro de datos 45
17.8. Certificación de fabricante requerida – Servidor para Data Center 46
18. ACUERDOS DE NIVELES DE SERVICIO (ANS) 46
18.1. Horas de Servicio por Compensación (Bolsa de Horas por Demanda) 46
18.2. Naturaleza de las Horas de Servicio 46
18.3. Características del Servicio 47
18.4. Tipología de Actividades Ejecutables 47
18.5. Activación y Gestión 48
18.6. Control y Trazabilidad 48
18.7. Vigencia 48
18.8. Descripción de ANS por línea de servicio 48
18.8.1. Renovación de soporte y garantía de la infraestructura tecnológica de Data Center alterno DCA 48
18.8.2. Suministro e implementación de los componentes para Data Centers DCP y NVC 50
19. ACUERDOS DE CONFIDENCIALIDAD 50
GLOSARIO 51

1. DESCRIPCIÓN DE LA NECESIDAD

De acuerdo con el Artículo 2.2.9.1.1.3. del Decreto 1008 de 2018 del Departamento Administrativo de la Función Pública, la política de Gobierno Digital se encuentra fundada en principios que rigen el sector de las TIC, como lo son: El de la Innovación, que propende por la introducción de soluciones novedosas que resuelven problemáticas haciendo uso de las Tics. La Competitividad, a través de la aplicación de este principio se busca optimizar la gestión pública a través de la generación de procesos ágiles y coordinados. La Proactividad, trabajo conjunto previo a la toma de decisiones para mitigar riesgos y atender necesidades, restableciendo confianza a través del uso de Tics. Seguridad de la Información, Confiabilidad, integridad y disponibilidad de la información.

Así mismo, en cumplimiento del Plan de Desarrollo Distrital “Bogotá Camina Segura”, adoptado mediante el Acuerdo 927 de 2024, y en el marco del componente de implementación de Tecnologías de la Información y las Comunicaciones (TIC) en las entidades distritales, la Secretaría de Educación del Distrito –SED– busca fortalecer su liderazgo tecnológico, alineándose con estándares y mejores prácticas del sector. El objetivo es consolidar un activo tecnológico robusto, sustentado en principios de seguridad digital, eficiencia operativa y alta disponibilidad, que garantice la continuidad y calidad de los servicios TIC que soportan la misión educativa de la entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), dependencia adscrita al despacho de la Secretaría de Educación del Distrito, informa mediante el presente documento la necesidad y justificación para la renovación de las garantías de los elementos de infraestructura tecnológica instalada en el Data Center localizado en el Centro para la Transformación Digital OTIC, así como el suministro e implementación de los componentes requeridos para el fortalecimiento del Data Center principal (DCP) y del nivel central (NVC), que forma parte de la ejecución del Proyecto de Inversión 7949: “Fortalecimiento y modernización de los sistemas de información, incluyendo innovación tecnológica, al servicio de la calidad educativa en los colegios públicos de la ciudad de Bogotá D.C.”, en el marco del Plan Distrital de Desarrollo (PDD) “Bogotá Camina Segura 2024–2027”.

De acuerdo con lo establecido en el Artículo 13 del Decreto 650 de 2025, la OTIC cumple un rol estratégico en la Secretaría de Educación del Distrito al orientar y asesorar la gestión integral de las TIC y la transformación digital, en concordancia con las políticas nacionales, sectoriales e institucionales. Su función se centra en fortalecer el uso eficiente de la información, impulsar el mejoramiento continuo de los procesos y contribuir al cumplimiento de la misión institucional. Para ello, participa activamente en los comités de alta dirección y asesora la planeación, evaluación y adopción de tecnologías en los niveles Central, Local e Institucional, promoviendo el uso de estándares, buenas prácticas y tecnologías de punta.

Asimismo, la OTIC es responsable de definir e implementar lineamientos para la adquisición, operación y sostenibilidad de la infraestructura tecnológica, los bienes y servicios TIC, garantizando su alineación con el Plan Sectorial de Desarrollo, el PETI y los estándares nacionales e internacionales. Entre sus funciones clave se encuentran la administración y operación de la infraestructura de cómputo, comunicaciones y Data Center; la prestación de servicios de soporte y mantenimiento de plataformas, aplicaciones y sistemas de información; la implementación de la arquitectura institucional y de los modelos de seguridad, privacidad e informática; y la provisión de servicios digitales seguros y confiables para usuarios internos y externos, en cumplimiento de la normatividad vigente.

El efecto dinamizador de las TIC no es ajeno al Sector Educación, su uso, con la guía de docentes comprometidos, permite a la niñez y a la juventud participar en los procesos de generación de conocimiento y desarrollar capacidades analíticas que les permitan enfrentarse a los nuevos retos de la sociedad del conocimiento. La gestión y mantenimiento de la infraestructura de TIC, al servicio de la educación, hacen parte de la estrategia que busca reducir la brecha tecnológica. Así mismo, dicha estrategia busca mejorar las condiciones de calidad de los procesos pedagógicos, motivar la permanencia y continuidad de los estudiantes en el ciclo de aprendizaje, con entornos de trabajo y estudio seguros tanto en lo presencial como lo digital y virtual fortaleciendo el carácter público de la educación.

Las necesidades de la Secretaría de Educación del Distrito exigen una adecuada gestión informática, un monitoreo continuo y la implementación de mejores prácticas de uso tecnológico, en aras de que la plataforma tecnológica que actualmente soporta estos procesos sea estable, eficiente, de alto desempeño y disponibilidad, minimizando las interrupciones en el servicio, manteniendo un alto estándar de calidad, continuidad y disponibilidad de todos los servicios que la entidad presta a sus usuarios, mediante la administración de las aplicaciones, la automatización de labores de administración, diagnóstico y solución de problemas.

La SED se ha centrado en la implementación de tecnologías de información del siglo XXI para sustentar la toma de decisiones, contando con sistemas de información integrados que contribuyan a optimizar los servicios en condiciones de eficiencia, para el presente caso.

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC de la Secretaría de Educación del Distrito (SED) en su compromiso con el cierre de la brecha digital y el apoyo a los procesos Administrativos a través del uso de las TIC a nivel central, local e institucional, tiene la responsabilidad de brindar los servicios de acceso a Internet y la disponibilidad de cada una de las aplicaciones web de uso interno y externo de la SED así como el de proteger el acceso a la información y los servicios informáticos entregados y usados por la entidad.

La Oficina de Tecnologías de Información y Comunicaciones – OTIC, ha implementado servicios tecnológicos en infraestructura híbrida que incluyen computación en nube (Cloud) compartida con servicios en sitio (Onpremise), en respuesta al hecho de que esta tecnología está evolucionando a una solución amplia de servicios TIC, ofrecidos por un importante número de proveedores de servicios en la Nube (PSN), con ofertas IaaS (infraestructura como servicio), PaaS (plataforma como servicio) y SaaS (software como servicio), además al observar que las implementaciones de 5G están haciendo su arribo a nuestro medio, los ecosistemas de nubes híbridas aprovecharán cada vez más las oportunidades para su adopción, con impacto directo en la optimización de costos, en la reducción en los tiempos de procesamiento y haciendo posible el ofrecimiento de nuevos y mejores servicios tecnológicos.

En predio ubicado en la Zona Industrial de Montevideo, Calle 17 No. 68 - 83, de propiedad de la SED, se encuentra el Centro para la Transformación Digital, el cual, mediante la ejecución del contrato CO1.PCCNTR. 5432493 de 2023, cuyo objeto es "*SUMINISTRO, INSTALACION Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA TECNOLÓGICA PARA EL DATA CENTER,* permitió adquirir la dotación de la estructura y las condiciones físicas y ambientales necesarias para soportar la infraestructura tecnológica y las áreas de servicio y de gestión del Data Center alterno.

En resumen, la necesidad se detalla en los siguientes tres componentes:

1.1. Renovación de soporte y garantía de la infraestructura tecnológica de Datacenter Alterno DCA

Los componentes de infraestructura de Data Center Alterno han contado con garantía y soporte de fábrica, servicios próximos a finalizar; lo que hace necesaria la contratación de una firma especializada en la prestación de los servicios de soporte y garantía con suministro de partes, para los elementos de infraestructura relacionados en la siguiente tabla:

TABLA 1. INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA DATA CENTER ALTERNO

#	Componente	Marca	Cantidad	Descripción	# Serie
1	FM2000	HUAWEI	1	Módulo compuesto por 8 racks de IT, el módulo ECC800, 3 racks de aire de precisión inrow y 2 racks de PDUs, 1 rack disponible para ampliación de aire acondicionado. 3 unidades NetCol500 (módulos exteriores de enfriamiento inteligente para la gestión térmica en racks).	Múltiples componentes
3	CloudEngine 6866-8S8CQ-P	HUAWEI	8	Switches TOR 1 unidad instalada en cada uno de los racks IT.	1023B5096944 1023A6441588 1023B5096956 1023A6441566 1023B5096947 1023B5096969 1023A6441594 1023B5096948
4	XPON V2804DAC	VSOL	16	Corresponde a los 64 puntos de red GPON instalados en CTD	V24042818026 V24042818035 V24042818040 V24042818031 V24042817625 V24042818033 V24042817615 V24042818034 V24042818027

#	Componente	Marca	Cantidad	Descripción	# Serie
					V24042818030 V24042818039 V24042818042 V24042818032 V24042818029 V24042818041 V24042817024
5	GPON OLT V1600GS	VSOL	1	OLT que administra y conecta la red GPON al anillo TOR.	V24042817045
6	Sistema de detección y extinción de incendios y control de alarma	Detección EDWARDS Extinción SEVO Alarma KIDDE	1	Sistema compuesto por los detectores de humo, sirenas estrambóticas, estación manual de alarmas, detector fotoeléctrico, interruptor de flujo, interruptor de supervisión, campana, cilindro contenedor de agente limpio y módulo de relevo de descarga.	Múltiples componentes
7	Planta eléctrica J150U_220	KOHLER	1	Planta eléctrica modificada en su tanque de reserva para una capacidad total de 250 galones de combustible.	22003111

Con base en la relación de elementos de la TABLA 1, la SED requiere contar con un proveedor especializado, que tenga la capacidad técnica, logística, financiera, el personal con el conocimiento y la experiencia suficiente, que le permitan garantizar la ejecución.

1.2. Fortalecimiento de la Infraestructura tecnológica de Datacenter Principal DCP

El Data Center Principal (DCP) requiere el fortalecimiento de sus condiciones ambientales y de protección eléctrica mediante módulos integrados tipo micro Data Center, con el fin de garantizar condiciones técnicas adecuadas para la infraestructura hiperconvergente instalada.

1.3. Fortalecimiento infraestructura de Datacenter NVC

En Nivel Central (NVC) se identifica la necesidad de fortalecer los servicios de Directorio Activo -AD y Protocolo de Configuración Dinámica de Host -DHCP mediante la incorporación de un servidor empresarial que permita mejorar la redundancia, disponibilidad y resiliencia de los servicios de autenticación y gestión de red.

La renovación del soporte y garantía del DCA no constituye una mejora tecnológica ni una ampliación de capacidad, sino una acción de aseguramiento orientada al mantenimiento de la infraestructura en condiciones óptimas de funcionamiento, conforme a estándares del fabricante y mejores prácticas de gestión de servicios TIC (ITIL).

Por su parte, el fortalecimiento del DCP y del NVC responde a la necesidad de:

- Mitigar riesgos asociados a condiciones ambientales no controladas.
- Garantizar continuidad de servicios críticos de red y autenticación.
- Optimizar la disponibilidad de la infraestructura hiperconvergente.
- Reducir la probabilidad de fallas sistémicas.
- Proteger la inversión pública realizada en activos tecnológicos estratégicos.

Estas acciones permiten consolidar una arquitectura tecnológica resiliente, alineada con esquemas de nube híbrida y recuperación ante contingencias.

En consecuencia, la renovación de soporte y garantía del Data Center Alterno (DCA), así como el fortalecimiento del Data Center Principal (DCP) y del Nivel Central (NVC), constituyen acciones necesarias para garantizar:

- Continuidad operativa.
- Alta disponibilidad de servicios tecnológicos.
- Fortalecimiento en la capacidad de recuperación ante desastres (DRP).
- Protección de la inversión pública en infraestructura crítica.
- Cumplimiento de estándares de seguridad digital y resiliencia tecnológica.

En resumen, con los argumentos expuestos, se hace necesario realizar un proceso de contratación con los siguientes componentes de infraestructura de la Secretaría de Educación del Distrito:

- Realizar la renovación y extensión del soporte y garantía de la infraestructura tecnológica del Data Center alterno (DCA).
- Suministrar e implementar los componentes requeridos para el fortalecimiento del Data Center principal (DCP).

- Suministrar e implementar los componentes requeridos para el fortalecimiento del Data Center de Nivel Central (NVC).

1. OBJETO

REALIZAR LA RENOVACIÓN Y EXTENSIÓN DEL SOPORTE Y GARANTÍA DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DATA CENTER ALTERNO (DCA), ASÍ COMO EL SUMINISTRO E IMPLEMENTACIÓN DE LOS COMPONENTES REQUERIDOS PARA EL FORTALECIMIENTO DE LOS DATA CENTER DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO.

2. ALCANCE DEL SERVICIO

El contratista deberá realizar el cumplimiento del objeto contractual mediante el desarrollo integral de la renovación de soporte y garantía de la infraestructura tecnológica de Datacenter Alterno DCA, así como el suministro e implementación de los componentes requeridos para el fortalecimiento del Data Center principal (DCP) y del nivel central (NVC) de la Secretaría de Educación del Distrito, a continuación de desarrolla el alcance específico.

NOTA:

El contratista deberá radicar el cronograma detallado bajo el formato diagrama de Gantt dentro de los quince (15) días calendario posteriores a la firma del acta de inicio.

2.1. Renovación de soporte y garantía de la infraestructura tecnológica de Datacenter Alterno DCA

Prestar los servicios de extensión de garantía para cada uno de los componentes listados, incluyendo como mínimo:

- Cobertura integral de partes, repuestos originales y mano de obra.
- Soporte técnico especializado conforme a los acuerdos de niveles de servicio (ANS) definidos en este anexo.
- Ejecución de mantenimientos preventivos y correctivos según la naturaleza de cada componente.
- Atención en sitio en las instalaciones de la Secretaría de Educación del Distrito.
- Acceso a actualizaciones de licenciamiento de firmware y software autorizadas por el fabricante.
- Elaboración y entrega de informes técnicos detallados posteriores a cada intervención.
- Personal técnico con certificación expedida por el fabricante o por el representante de la marca en Colombia.

El servicio deberá contar con disponibilidad y prestarse durante un (1) año de ejecución contractual.

2.2. Fortalecimiento de la Infraestructura tecnológica de Datacenter Principal DCP

El contratista deberá realizar el suministro e instalación siete (7) módulos integrados tipo microcentro de datos "todo en uno" que integre UPS, distribución de energía, refrigeración, monitoreo, baterías y sistema

de extinción de incendios dentro de un solo gabinete cerrado, para permitir la instalación en sitio y proteger la infraestructura hiperconvergente de Datacenter Principal con aire acondicionado de precisión y Sistema de detección y extinción de incendios.

Cada uno de los módulos deberá:

- Garantizar condiciones ambientales óptimas para infraestructura hiperconvergente.
- Cumplir normativa RETIE y estándares técnicos aplicables.
- Entregarse instalado, configurado y probado.
- Incluir documentación técnica, manuales y acta de puesta en operación.

2.3. Fortalecimiento infraestructura de Datacenter NVC

El contratista deberá realizar el suministro de un (1) servidor para fortalecer los servicios de Protocolo de Configuración Dinámica de Host – DHCP y Directorio Activo – AD en Nivel Central

- Realizar la instalación en rack y conectado a fuentes de energía y DHCP.

La entidad cuenta con Licenciamiento y un equipo de soporte de infraestructura tecnológica con profesionales especializados que realizaran la instalación de Sistema Operativo y la configuración y activación de los servicios Directorio Activo y DHCP.

3. CÓDIGOS UNSPSC

El presente proceso se encuentra enmarcado dentro de los siguientes códigos del clasificador de bienes y servicios UNSPSC:

TABLA 3. Códigos UNSPSC

Clasificación UNSPSC	Segmento		Familia		Clase	
43222600	43	Difusión de Tecnologías de Información y Telecomunicaciones	22	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	26	Equipo de servicio de red
43232800	43	Difusión de Tecnologías de Información y Telecomunicaciones	23	Software	28	Software de administración de redes
43233200	43	Difusión de Tecnologías de Información y Telecomunicaciones	23	Software	32	Software de seguridad y protección

Clasificación UNSPSC	Segmento		Familia		Clase	
81111500	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	15	Ingeniería de software o hardware
81111800	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	18	Servicios de sistemas y administración de componentes de sistemas
81112200	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	22	Mantenimiento y soporte de software
26111600	**26**	**Maquinaria y accesorios de generación y distribución de energía**	**11**	**Baterías, generadores y transmisión de energía cinética**	**16**	**Generadores de energía (plantas eléctricas o grupos electrógenos)**
39121000	**39**	**Equipos y componentes eléctricos**	**12**	**Equipo de distribución y potencia**	**10**	**Equipamiento para distribución y conversión de alimentación**
39121600	**39**	**Equipos, suministros y componentes eléctricos.**	**12**	**Equipos de distribución y control eléctrico.**	**16**	**Dispositivos y accesorios para la protección de circuitos.**

4. DESCRIPCIÓN DE LA RENOVACIÓN DE SOPORTE Y GARANTÍA

El contratista está obligado a ejecutar al menos dos (2) mantenimientos preventivos anuales, separados con mínimo 4 meses entre el primer y segundo mantenimiento.

La infraestructura tecnológica del Data Center Alterno de la SED descrita en la Tabla 1, constituye un activo estratégico para la continuidad operativa, la resiliencia institucional y la disponibilidad de los servicios digitales que soportan la prestación del servicio público educativo en Bogotá.

Este inventario evidencia una arquitectura tecnológica moderna basada en componentes de misión crítica, dentro de los que se destacan:

- Infraestructura modular de alta densidad (Huawei FM2000) con sistemas integrados de energía, enfriamiento y gestión inteligente.
- Capa de red de alto desempeño (switches TOR Huawei CloudEngine) que soporta la conectividad interna de los racks de cómputo.

- Infraestructura GPON (VSOL OLT + ONTs) para distribución eficiente de conectividad.
- Sistemas de soporte vital del Data Center, incluyendo:
  - Sistema de detección y extinción de incendios (EDWARDS, SEVO, KIDDE).
  - Planta eléctrica KOHLER con autonomía extendida.

5.1. Criticidad de la Infraestructura.

Los componentes identificados no son elementos aislados, son parte de un ecosistema altamente integrado cuya indisponibilidad puede generar:

- Interrupción de servicios digitales misionales y de apoyo (matrículas, apoyo escolar, movilidad escolar, sistema financiero Apoteosys, nómina, correo electrónico, gestión documental).
- Afectación de la operación administrativa y financiera.
- Riesgos reputacionales e institucionales.
- Incumplimientos normativos en materia de continuidad y seguridad de la información.

5.2. Complejidad Tecnológica y Especialización.

Los equipos instalados corresponden a tecnologías especializadas que requieren:

- Conocimiento certificado por fabricante (Huawei, VSOL, KOHLER, EDWARDS, SEVO, KIDDE).
- Herramientas propietarias de diagnóstico y mantenimiento.
- Acceso a firmware, parches y actualizaciones oficiales.
- Capacidades avanzadas en gestión térmica, eléctrica y de redes de alta velocidad.

La operación sin respaldo especializado incrementa significativamente el riesgo de fallas no detectadas, configuraciones inadecuadas o tiempos prolongados de recuperación.

5.3. Necesidad de Soporte con Suministro de Partes.

Dado que varios componentes son de alta criticidad y operación continua (24/7), es indispensable contar con:

- Atención especializada.
- Suministro oportuno de repuestos originales, reduciendo tiempos de importación.
- Mantenimiento preventivo y correctivo certificado.
- Monitoreo de eventos.
- Acompañamiento en evolución tecnológica y optimización de la infraestructura.

5.4. Alineación con Buenas Prácticas

La contratación de estos servicios se alinea con marcos de referencia como:

- ITIL (gestión de servicios TI).

- ISO/IEC 27001 (seguridad de la información).
- ISO 22301 (continuidad del negocio).
- Recomendaciones de fabricantes para operación de infraestructura crítica.

NOTA:

Para la Planta Eléctrica J150U_220, el servicio de mantenimiento incluye:

a. Mantenimiento preventivo
b. Revisión y diagnóstico integral de motor, alternador y panel de control
c. Pruebas de carga y operación controlada
d. Inspección de sistemas de combustible, escape, refrigeración y lubricación
e. Documentación y gestión de la garantía del fabricante
f. Reemplazo de consumibles y repuestos aprobados por el fabricante
g. Asistencia prioritaria ante fallas o alarmas del sistema

Para los demás ítems, la renovación y extensión de garantía corresponde a la contratación de un servicio especializado mediante el cual la Secretaría de Educación del Distrito asegura, por un período adicional de doce (12) meses, la cobertura técnica, operativa y administrativa de los componentes de infraestructura tecnológica instalados en el Data Center Alterno del Centro para la Transformación Digital (CTD).

Desde el punto de vista técnico, la extensión de garantía implica:

- La continuidad de la cobertura del fabricante o de un canal autorizado, garantizando que cualquier intervención sobre los equipos se realice bajo estándares certificados y conforme a las especificaciones originales de diseño.
- La disponibilidad de repuestos originales o equivalentes certificados, eliminando el riesgo de incompatibilidades, degradación del desempeño o afectación de la vida útil de los activos.
- El acceso a actualizaciones de firmware, parches de seguridad y recomendaciones técnicas, indispensables para mantener los niveles de estabilidad, seguridad y soporte de los sistemas de energía, climatización, red, seguridad y cómputo.
- La atención de incidentes mediante soporte técnico especializado, con tiempos de respuesta y restauración acordes a la criticidad de los servicios soportados por el Data Center Alterno.
- La ejecución de mantenimientos preventivos programados, orientados a la detección temprana de fallas, reducción de eventos disruptivos y preservación de las condiciones óptimas de operación.

NOTA: Toda marca o referencia técnica descrita se entiende seguida de la frase "o equivalente", siempre que supere o iguale las condiciones técnicas exigidas.

Desde el punto de vista administrativo y contractual, la extensión de garantía:

- Constituye una obligación legal y técnica derivada del principio de planeación, en tanto la Entidad debe prever la continuidad del soporte una vez finalizada la garantía inicial de los bienes adquiridos.
- Permite a la SED proteger la inversión pública realizada, evitando costos extraordinarios asociados a reparaciones no cubiertas, reposición anticipada de equipos o contratación de servicios correctivos de emergencia.
- Facilita el control, supervisión y seguimiento contractual, al establecer un único responsable por la atención de fallas, suministros de repuestos y cumplimiento de los niveles de servicio.
- Reduce la exposición a riesgos operativos, financieros y reputacionales, derivados de la indisponibilidad del Data Center Alterno que soporta los sistemas misionales y de apoyo de la Entidad.
- Garantiza el cumplimiento de los deberes de conservación, custodia y uso eficiente de los bienes del Estado, exigidos por la normativa de contratación pública y por los organismos de control.

En este contexto, la renovación y extensión de garantía no constituye una mejora o actualización de la infraestructura existente, sino un mecanismo de aseguramiento técnico y administrativo, orientado a mantener la infraestructura en condiciones óptimas de funcionamiento, preservando la continuidad del servicio público de educación y la capacidad de recuperación institucional ante eventos de falla o contingencia.

Con alineación con las buenas prácticas ITIL y con la criticidad del Data Center Alterno del CTD de la SED, la siguiente es la Clasificación de Niveles de Severidad de Incidentes:

Tabla 4. Clasificación de Niveles de Severidad de Incidentes

Nivel de Severidad	Denominación	Descripción del Incidente	Impacto en la Operación de la SED	Ejemplos de Incidentes
1	Crítica	Incidente que genera indisponibilidad total o pérdida severa de funcionalidad de la infraestructura crítica del Data Center Alterno, sin solución de contingencia inmediata.	Afectación directa a los respaldos de los sistemas misionales y de apoyo que soportan la prestación del servicio público de educación. Riesgo alto de indisponibilidad de procesos institucionales críticos.	• Caída total del Data Center Alterno. • Indisponibilidad del core de red switch TOR. • Activación o falla del sistema de detección/extinción de incendios. • Pérdida total de conectividad hacia sistemas críticos.
2	Alta	Incidente que afecta parcialmente la operación de la infraestructura crítica o degrada de forma significativa el desempeño de los servicios, con	Afectación relevante de los respaldos de procesos misionales o de apoyo, con riesgo de escalar a indisponibilidad total si no se atiende oportunamente.	• Falla de uno o más switches de core o distribución con impacto en redundancias. • Fallas intermitentes de climatización.

Nivel de Severidad	Denominación	Descripción del Incidente	Impacto en la Operación de la SED	Ejemplos de Incidentes
		alternativas temporales limitadas.		• Degradación severa de enlaces de red (switches TOR) • Alarmas críticas persistentes en sistemas de monitoreo.
3	Media	Incidente que afecta componentes no críticos o redundantes, sin generar interrupción del servicio, pero que requiere corrección para evitar escalamiento.	Impacto bajo o controlado sobre la operación institucional, sin afectación directa, pero con riesgo potencial si no se corrige.	• Falla de un equipo en configuración redundante sin pérdida de servicio. • Alertas de capacidad o desempeño fuera de umbral. • Fallas de componentes secundarios (ventiladores, fuentes redundantes).
4	Baja	Incidente menor que no afecta la operación ni el desempeño de los servicios y puede ser atendido en ventanas programadas.	Sin impacto en la continuidad de los respaldos de procesos misionales ni administrativos de la SED.	• Solicitudes de información técnica. • Ajustes menores de configuración. • Actualizaciones de firmware no críticas. • Consultas de operación o mantenimiento.

Tabla 5. Tiempo de respuesta ante Incidentes

Nivel de Severidad	Denominación	Tiempo de Respuesta Estimado	Cobertura Horaria
1	Crítica	≤ 2 hora	24x7
2	Alta	≤ 4 horas	24x7
3	Media	≤ 12 horas	Horario laboral estándar
4	Baja	≤ 24 horas	Horario laboral estándar

El contratista deberá garantizar el cumplimiento estricto de los tiempos de respuesta establecidos para la atención de incidentes, conforme al nivel de severidad asignado, para lo cual deberá disponer de los recursos técnicos y humanos necesarios que garanticen el cumplimiento de estos tiempos de atención y aseguren la continuidad operativa de la infraestructura.

NOTA: En aquellos eventos en que el fabricante de un determinado componente, equipo, software o solución tecnológica establezca condiciones de atención, tiempos de respuesta o Acuerdos de Niveles de Servicio (ANS) propios para la prestación de los servicios de garantía, soporte o mantenimiento, estos serán aplicables en lo que corresponda, siempre que se encuentren debidamente acreditados y no sean consecuencia de una actuación u omisión imputable al contratista. En tales casos, prevalecerán las condiciones definidas por el fabricante para la atención del respectivo incidente o requerimiento, sin que ello implique incumplimiento por parte del contratista respecto de los ANS contractuales, en la medida en que dichos tiempos obedezcan a procedimientos o políticas técnicas propias del fabricante y escapen al ámbito de control del contratista.

5. DESCRIPCIÓN DEL SUMINISTRO E IMPLEMENTACIÓN DE COMPONENTES PARA LOS DATA CENTER

A continuación, se presenta la descripción para realizar el suministro e implementación de componentes requeridos para el fortalecimiento de los Data Center de la Secretaría de Educación del Distrito (**DCP y NVC)**.

Requerimientos de Energía Eléctrica:

Los equipos deben operar a un voltaje nominal de 208 V o 220 V entre fases (y 120 V entre fase y neutro), compatibles con las PDU instaladas en los racks del Data Center de la SED.

Especificaciones de Temperatura y Humedad:

El hardware ofertado debe operar sin degradación de rendimiento dentro de los rangos estándar de ASHRAE para Data Centers (Temperatura de 18°C a 27°C y Humedad Relativa del 40% al 55%).

Estándares de Seguridad:

Los equipos ofertados deben cumplir con certificaciones internacionales estándar de seguridad y compatibilidad electromagnética como CE, UL y FCC.

5.1. MÓDULOS INTEGRADOS TIPO MICRO CENTRO DE DATOS

5.1.1. Protección integral de la infraestructura hiperconvergente del DCP

La SED opera una infraestructura hiperconvergente de misión crítica que soporta:

- Sistemas misionales del servicio público educativo.
- Plataformas administrativas y financieras.
- Servicios de autenticación y control de identidad.
- Integraciones híbridas con servicios en la nube.

Dicha infraestructura requiere condiciones estrictas de:

- Disponibilidad eléctrica continua (alta resiliencia energética).
- Control térmico de precisión.

- Monitoreo ambiental y eléctrico permanente.
- Sistema de detección y extinción de incendios.

Actualmente, los riesgos asociados a fallas eléctricas, variaciones térmicas o eventos de incendio pueden comprometer:

- La continuidad del servicio educativo distrital.
- La integridad de la información institucional.
- La reputación institucional y cumplimiento normativo.

La adquisición de siete (7) módulos integrados tipo micro centro de datos “todo en uno” responde a un enfoque de:

- Contención física especializada.
- Microclimatización controlada.
- Integración de UPS, baterías y distribución eléctrica certificada RETIE.
- Sistema autónomo de detección y extinción.

Este modelo reduce la dependencia de infraestructura civil compleja y permite:

- Implementación modular y escalable.
- Disminución del MTTR (Mean Time To Repair).
- Segmentación de cargas críticas.
- Aumento del nivel de resiliencia del Data Center Principal.

Desde una perspectiva de arquitectura TI, el esquema propuesto fortalece la capa física (Layer 0) sobre la cual opera la plataforma hiperconvergente, alineándose con buenas prácticas de diseño de Data Centers satisfaciendo las necesidades de aire acondicionados de precisión, condiciones físicas, ambientales, sistema de detección y extinción de incendios en procura de optimizar el funcionamiento y extender la vida útil de la infraestructura tecnológica.

5.2. SERVIDOR PARA DIRECTORIO ACTIVO Y DHCP EN NVC

5.2.1. Fortalecimiento de servicios de Directorio Activo y DHCP en NVC

El servidor requerido para Nivel Central tiene carácter estratégico, dado que soporta:

- Servicios de Directorio Activo (AD).
- Protocolo de configuración dinámica de host DHCP.
- Autenticación y resolución de identidad.
- Políticas de seguridad.

El Directorio Activo constituye la columna vertebral de autenticación institucional. Una degradación de este servicio impactaría:

- Inicio de sesión de funcionarios.
- Acceso a sistemas misionales.
- Servicios en la nube.
- Aplicaciones internas.

El nuevo servidor permitirá:

- Incrementar redundancia.
- Mejorar tiempos de respuesta.
- Distribuir carga.
- Fortalecer la disponibilidad en Nivel Central.
- Reducir puntos únicos de falla.

Es importante resaltar que la entidad ya cuenta con:

- Licenciamiento requerido.
- Equipo técnico especializado para despliegue.
- Capacidad de configuración interna.

Por lo tanto, este ítem se limita al suministro e instalación física, sin incurrir en costos de servicios profesionales que la entidad está en capacidad de ejecutar con talento propio.

Para los componentes requeridos para el fortalecimiento de los Data Center (**DCP y NVC)**, el contratista está obligado a ejecutar al menos dos (2) mantenimientos preventivos anuales, separados con mínimo 4 meses entre el primer y segundo mantenimiento. El alcance de los mantenimientos preventivos incluye limpieza interna/externa, verificación de alertas de hardware, actualización preventiva de microcódigo y pruebas de diagnóstico de componentes.

6. LUGAR DE ENTREGA

Los bienes y servicios definidos en el presente documento deberán ser entregados de la siguiente manera:

- Renovación de soporte y garantía de la infraestructura tecnológica de Datacenter Alterno DCA.
  En CTD Centro para la Transformación Digital OTIC.
  Dirección: Calle 17 # 68 - 83 Zona Industrial Montevideo.

- Fortalecimiento de infraestructura de Datacenter de Nivel Central
  En NVC Nivel Central de la Secretaría de Educación del Distrito
  Dirección: Avenida el Dorado # 66-63 Piso 2.

- Fortalecimiento de la Infraestructura tecnológica de Datacenter Principal DCP.
  En CDI Centro de Innovación Saber Digital OTIC.
  Dirección: Carrera 28A # 62-46 Piso 2.

NOTA: Cualquier cambio, actualización o variación en la nomenclatura urbana en la ubicación de los Datacenter, no afectará ni modificará el lugar de ejecución contractual aquí pactado.

7. PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato será hasta el 31 de diciembre de 2026, el cual será contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución, término dentro del cual deberán ejecutarse la totalidad de las obligaciones a cargo del contratista, así:

1. Renovación y extensión del soporte y garantía de la infraestructura tecnológica del Data Center Alterno – DCA (Tabla 1). El contratista deberá entregar y activar la renovación y extensión del soporte y la garantía dentro del plazo de ejecución del contrato. La cobertura del soporte y de la garantía será por el término de un (1) año contado a partir de su activación, sin que dicha cobertura amplíe el plazo de ejecución contractual.
2. Suministro e implementación de los componentes para el Data Center Principal – DCP. Para los siete (7) módulos integrados tipo micro centro de datos, hasta el 31 de diciembre de 2026, término dentro del cual deberán surtirse la entrega física a la SED, la instalación y configuración y el afinamiento.
3. Suministro e implementación del servidor para el Data Center de Nivel Central – NVC. Para el servidor destinado a los servicios de DHCP y Directorio Activo – AD, hasta el 31 de diciembre de 2026, término dentro del cual deberán surtirse la entrega física a la SED, la instalación y conexión.

8. FORMA DE PAGO

La Secretaría de Educación del Distrito, pagará el valor del contrato de la siguiente manera:

- Un primer pago previo a la RENOVACIÓN DE SOPORTE Y GARANTÍA DE LA INFRAESTRUCTURA TECNOLÓGICA DE DATACENTER ALTERNO - DCA, una vez se realice la renovación de garantía con el fabricante y se evidencie la actualización para la solución de DataCenter Alterno conforme a lo descrito en la (TABLA 1. INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA), junto con el recibido a satisfacción por parte de la supervisión. El monto de este pago corresponde al valor de este ítem de la oferta adjudicada.

- Un segundo pago una vez terminado el afinamiento del ítem SUMINISTRO E IMPLEMENTACIÓN DE LOS COMPONENTES PARA DATA CENTER PRINCIPAL DCP, junto con el recibido a satisfacción por parte de la supervisión.

- Un tercer pago una vez terminado la instalación y conexión del ítem SUMINISTRO E IMPLEMENTACIÓN DE SERVIDOR PARA DATA CENTER NIVEL CENTRAL NVC, previo recibido a satisfacción por parte de la supervisión.

El valor del contrato a suscribir será el resultante de la adjudicación, el cual incluye el IVA, así como todos los costos directos e indirectos asociados al suministro de los bienes y/o prestación del servicio y demás tributos de ley que se generen con ocasión de la celebración y ejecución del contrato.

Los pagos del contrato se efectuarán previa presentación de la factura o documento equivalente, con informe de ejecución y recibido a satisfacción por parte del supervisor del contrato, quien deberá verificar el cumplimiento en el pago de los aportes a la Seguridad Social Integral y parafiscales.

Los impuestos, tasas, contribuciones y retenciones que surjan del presente contrato serán sufragados por el contratista, para cuyos efectos se harán las retenciones del caso y se cumplirán las obligaciones fiscales que ordene la normatividad vigente.

PARÁGRAFO 1º: Dicha información será verificada por parte del Supervisor de la SED y se procederá a dar visto bueno para el trámite de la cuenta. El CONTRATISTA deberá cumplir con los requisitos de pago.

PARÁGRAFO 2º: Todo pago estará sujeto a la Programación Anualizada de Caja -PAC de la Dirección Distrital de Tesorería y a las fechas de pago establecidas por la SED, sin generar intereses moratorios.

PARÁGRAFO 3º: En el evento que el CONTRATISTA no presente la factura o su documento equivalente para el pago, estando obligado a ello de conformidad con el régimen tributario aplicable, la SED no lo tramitará mientras no se cumpla la obligación por parte del CONTRATISTA y en consecuencia el retraso en el pago que se produzca por esta circunstancia no generará interés moratorio alguno a cargo de la SED.

PARÁGRAFO 4º: En el evento de que algún pago sea objeto del proceso de Pasivo Exigible, la duración de este trámite presupuestal no ocasionará ningún tipo de responsabilidad, ni interés por parte de la SED a favor del contratista. Dicho pago estará sujeto al cumplimiento del procedimiento establecido en la Resolución No. SDH-000037 del 6 de marzo de 2019 expedida por la Secretaría Distrital de Hacienda, o la que se encuentre vigente.

PARÁGRAFO 5º: Para cada pago se debe presentar como soporte el acta de entrega y de recibo a satisfacción de los bienes y/o servicios objeto del contrato de acuerdo con el manual de contratación y/o manual de supervisión e interventoría de la SED, al concepto cobrado en forma independiente y anexando los demás requerimientos presupuestales y legales a que haya lugar.

PARÁGRAFO 6º: El CONTRATISTA deberá, al momento del pago, diligenciar el formato exigido por la Dirección Financiera de la SED, con el fin de proporcionar la información necesaria para la realización de los pagos por parte de la Secretaría de Educación del Distrito Capital, los cuales se harán por medio del Sistema Automático de Pagos S.A.P.

PARÁGRAFO 7º: Las variaciones que llegaren a suscitarse dentro del desarrollo del contrato, tendrán repercusión en las fechas previstas para los pagos programados con cargo al mismo.

PARÁGRAFO 8º. Cumplir con todos y cada uno de los aspectos señalados en el procedimiento, implementado mediante la Resolución No. SDH-000191 del 22 de septiembre de 2017, modificada por la Resolución No. 37 de 2019, expedida por la Secretaría Distrital de Hacienda, o la que se encuentre vigente.

NOTA: En implementación a la Ley 2024 de 2020 - “Ley de pagos a plazos justos”, del Decreto Reglamentario 1733 de 2020 y del Decreto Distrital 640 de 2025; el plazo de pago a contratistas será máximo de treinta (30) días calendario luego de recibido el bien o servicio que determine la cláusula contractual, siempre y cuando se cuente con el recibo a satisfacción por parte del supervisor o interventor y con el cumplimiento de todos los demás requisitos que correspondan a cargo del contratista.

9. SERVICIOS DE SOPORTE

- Para la prestación del servicio de soporte para el inventario de elementos de infraestructura Data Center alterno (TABLA 1) el contratista deberá realizar las gestiones necesarias ante los fabricantes para asegurar que las garantías renovadas queden activas y tengan vigencia de un (1) año contado a partir de la suscripción del acta de inicio, presentando constancia formal de dicha activación y evidenciando en la plataforma de soporte del fabricante.

    - El contratista deberá entregar en el sitio designado por la entidad (Bogotá D.C.) la renovación soporte y extensión de garantía, en las condiciones descritas en el presente Anexo Técnico y disponer de los recursos físicos, lógicos y administrativos para el cumplimiento del contrato.

- Para la prestación del servicio de soporte para los componentes de Data Centers DCP y NVC suministrados, el contratista deberá realizar las gestiones necesarias ante los fabricantes para asegurar que las garantías renovadas queden activas y tengan vigencia de tres (3) años contados a partir del recibido a satisfacción por parte de la entidad, presentando constancia formal de dicha activación y evidenciando en la plataforma de soporte del fabricante.

    - El contratista deberá entregar en el sitio designado por la entidad (Bogotá D.C.) soporte y la garantía, en las condiciones descritas en el presente Anexo Técnico y disponer de los recursos físicos, lógicos y administrativos para el cumplimiento del contrato.

De manera integral el soporte provisto por el contratista deberá contemplar los siguientes requisitos:

- Dentro de los cinco (5) días hábiles siguientes a la firma del acta de inicio, el contratista deberá entregar a la entidad la documentación formal con la información completa sobre las líneas de atención, protocolos de escalamiento, tiempos de respuesta y canales habilitados para acceder al soporte de fábrica en modalidad 24x7x365, incluyendo número de caso, niveles de prioridad y contacto del fabricante.
- El contratista deberá disponer de canales electrónicos y telefónicos eficientes para la recepción y gestión de solicitudes de soporte técnico, los cuales deben incluir como mínimo un portal web habilitado para radicación de tickets, una cuenta de correo electrónico exclusiva para soporte y una línea telefónica directa o conmutador para la atención de incidentes críticos.
- Será obligación del contratista garantizar la trazabilidad, el seguimiento y el cierre documentado de cada incidente o solicitud de soporte, en articulación con el fabricante, manteniendo siempre informada a la supervisión del contrato sobre el avance y resolución de cada caso.
- Durante la ejecución del contrato, el Contratista deberá mantener vigente la membresía en el nivel presentado en su oferta, otorgada por el fabricante o su representante en Colombia, lo cual garantiza que el servicio especializado prestado por el Contratista cuenta con el aval del fabricante.
- Como parte del servicio, el contratista deberá realizar monitoreo proactivo de la infraestructura, emitiendo informes periódicos con alertas sobre eventos potenciales, recomendaciones de mejora técnica y acciones preventivas que permitan anticiparse a fallas o degradaciones del servicio.
- El contratista deberá garantizar la disponibilidad permanente del servicio de soporte técnico durante las 24 horas del día, los siete días de la semana, incluidos domingos y festivos, para la atención oportuna de cualquier incidente que pueda afectar la operación de la infraestructura.
- Deberá presentarse a la entidad un informe de soporte mensual que incluya el registro detallado de incidentes atendidos, tiempos de respuesta, acciones realizadas, actualizaciones implementadas en el periodo correspondiente.
- En caso de presentarse fallas clasificadas como críticas o de Gravedad 1 (establecida por el

fabricante), el contratista deberá gestionar de manera inmediata la atención prioritaria, incluyendo la intervención técnica especializada y la entrega de repuestos en sitio en un plazo no mayor a cuatro (4) horas, con el fin de restablecer la operación en el menor tiempo posible.

- Para efectos de la gestión y seguimiento a la solución de fallas, se precisa que la entidad cuenta con el Operador Tecnológico contratado por la entidad para la administración y operación de la infraestructura de Data Center.
- El contratista deberá brindar acompañamiento técnico en procesos de actualización de firmware, software o migración de componentes críticos, verificando la compatibilidad de versiones y asegurando la continuidad de los servicios durante la ejecución de estos cambios.
- Deberá garantizar el acceso oportuno a actualizaciones, parches de seguridad y mejoras recomendadas por el fabricante, aplicándolos conforme a las mejores prácticas de la industria y verificando que las configuraciones se mantengan alineadas con los criterios de seguridad, rendimiento y estabilidad requeridos por la entidad.
- El contratista deberá realizar las gestiones necesarias ante los fabricantes para asegurar que todas las garantías renovadas queden activas y tengan vigencia de un (1) año contado a partir de la suscripción del acta de inicio, presentando constancia formal de dicha activación y evidenciando en la plataforma de soporte del fabricante.

10. SERVICIOS DE RENOVACIÓN Y EXTENSIÓN DE GARANTÍA FABRICANTE PARA INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA DATA CENTER ALTERNO (TABLA 1.)

- El soporte del contratista incluye atención remota y en sitio ante fallas de hardware, reemplazo de partes averiadas, acceso a actualizaciones de firmware y parches de seguridad, así como escalamiento a ingenieros de segundo y tercer nivel según la severidad del incidente reportado. Este soporte debe garantizar la trazabilidad de cada caso mediante número de ticket, niveles de prioridad y comunicación directa con personal técnico del fabricante.
- La renovación y extensión de la garantía con vigencia de un (1) año contado a partir de la suscripción del acta de inicio. El contratista deberá garantizar que las garantías sean activadas correctamente, suministrar documentación completa de contacto y escalamiento y acompañar el proceso técnico cuando se requiera intervención conjunta.
- En caso de fallas críticas, el fabricante realizará la entrega de repuestos y personal técnico en sitio en un plazo máximo de cuatro (4) horas, asegurando la continuidad del servicio.

11. SERVICIOS DE GARANTÍA DE FABRICANTE PARA COMPONENTES DE DATA CENTERS DCP y NVC SUMINISTRADOS

De acuerdo con lo expresado en el Numeral 6. DESCRIPCION DEL SUMINISTRO E IMPLEMENTACIÓN DE COMPONENTES PARA LOS DATA CENTER, se requiere servicio de garantía directo por el fabricante en la modalidad 7x24x365, durante el periodo de tres (3) años, que incluye el reemplazo de partes, para las soluciones suministradas por el contratista, con plazo máximo al siguiente día calendario de ocurrencia de la falla.

Las soluciones ofertadas o componentes que requieran ser remplazados deben ser nuevos de fábrica, no remanufacturados, ni reparados, ni reacondicionados en ninguna de sus partes.

Las actualizaciones de software, firmware y parches / fixes de la solución ofertada, deben ser realizadas por el contratista en forma integrada y considerando la totalidad de componentes.

La atención se debe prestar dentro de las cuatro (4) horas siguientes al reporte de incidente. En el caso específico que la solución requiera de soporte de tercer nivel (fabricante), todas estas labores y demás actividades propias del soporte y garantía serán gestionadas por el contratista, quien deberá escalar gestionar y realizar todos los procedimientos que el fabricante solicite.

Durante el tiempo de garantía tres (3) años, se deberá prestar soporte de la solución con personal especializado en la plataforma ofertada, teniendo en cuenta el soporte del fabricante.

El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil.

El contratista deberá realizar y documentar, las siguientes actividades como parte de soporte:

- Revisar
- Diagnosticar
- Optimizar globalmente la solución.

El contratista deberá incluir la garantía de reemplazo de unidades completas, componentes, tarjetas, cables, accesorios o partes en la modalidad 7 x 24 x 365 durante el periodo de garantía para toda la solución ofertada. Las partes que sean reemplazadas por efecto de la garantía deben estar homologadas por el fabricante del equipo ofertado, deberán ser nuevos de fábrica, no remanufacturados, ni reparados, ni reacondicionados en ninguna de sus partes y de iguales o superiores condiciones técnicas a las reemplazadas.

Al finalizar cada visita correctiva y/o preventiva el contratista generará un informe de servicio en el que constará el resumen de las actividades realizadas (actualización y soporte), problemas presentados, soluciones utilizadas y recomendaciones, así como las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración.

El periodo de garantía inicia a partir del siguiente día del recibido a satisfacción por parte de la entidad.

12. GARANTÍAS

Con el fin de dar cumplimiento a lo establecido en el Artículo 7º de la Ley 1150 de 2007, y según lo dispuesto en el Decreto Nacional 1082 de 2015, la SED solicitará al futuro contratista, las garantías que cubran los siguientes amparos:

TABLA 6. AMPAROS

Amparo	Valor / Porcentaje	Vigencia
Cumplimiento	20% del valor total de contrato	Por el plazo de la renovación, es decir un (1) año y seis (6) meses más

Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5% del valor total del contrato	Por el plazo de la renovación, es decir un (1) año y tres (3) años más
Calidad del servicio	20% del valor total de contrato	Por el plazo de la renovación, es decir un (1) año y seis (6) meses más
Calidad y correcto funcionamiento de los bienes	20% del valor total de contrato	Por el plazo de la renovación, es decir un (1) año y seis (6) meses más
Póliza Responsabilidad Extracontractual	De conformidad con lo establecido en el artículo 2.2.1.2.3.1.17 del Decreto 1082 de 2015.	Por el plazo de ejecución del contrato

13. COMPONENTES OBJETO DE LA EXTENSIÓN DE GARANTÍA

El contratista está obligado a ejecutar al menos dos (2) mantenimientos preventivos anuales, separados con mínimo 4 meses entre el primer y segundo mantenimiento.

13.1. Sistema Modular de Data Center

- Equipo: Huawei FusionModule2000 (FM2000)
  Módulo compuesto por 8 racks de IT, el módulo ECC800, 3 racks de aire de precisión inrow y 2 racks de PDUs, 1 rack disponible para ampliación de aire acondicionado, con tres (3) unidades NetCol500 (módulos exteriores de enfriamiento inteligente para la gestión térmica en racks)
- Cantidad: 1
- Alcance mínimo:
  - Inspección eléctrica y mecánica integral.
  - Limpieza de filtros y verificación de eficiencia energética (PUE).
  - Pruebas funcionales de sensores, controladores, alarmas y sistema de monitoreo.
  - Actualización de firmware y controladores.
  - Verificación de parámetros térmicos y flujo de aire de los módulos de enfriamiento
  - Reemplazo de piezas defectuosas.

13.1.1. Especificaciones de soporte y garantía estándar integral para Sistema Modular Datacenter - FM2000

El proponente deberá garantizar la continuidad operativa de la solución FusionModule (FM2000) y sus componentes de precisión, bajo un esquema de responsabilidad total durante el periodo contratado.

A. Vigencia y Periodo de Cobertura

- Inicio de la Cobertura: A partir de la suscripción de acta de inicio.
- Duración: Un (1) año (12 meses).

- Alcance: Incluye el módulo FM2000 y el sistema de aire acondicionado de precisión FusionCol (InRow).

B. Responsabilidad Integral del Contratista

Cualquier evento, componente o servicio que sea rechazado o no esté cubierto por la política de garantía estándar de fábrica de Huawei deberá ser cubierto en su totalidad por el contratista, sin costo adicional para el cliente. Esto incluye, pero no se limita a:

- ANS y Tiempos de Respuesta: Si bien la fábrica ofrece un tiempo de 30 días laborables para repuestos (30BD-S), el contratista es responsable de gestionar el stock local o las medidas necesarias para asegurar la operatividad del sistema.
- Consumibles y Desgaste: El contratista asumirá el costo y reemplazo de los elementos excluidos por fábrica, tales como: refrigerantes, filtros de aire/agua, sensores de pH/conductividad, grasa térmica y tambores de humidificación.
- Software de Gestión: El contratista debe garantizar la funcionalidad del software NetEco durante los 12 meses de contrato.
- Independientemente de la denominación comercial que el fabricante utilice para el software de gestión (verbigracia NetEco o la herramienta equivalente para la administración de dicha serie), es obligatorio contar con una plataforma que permita la visibilidad y administración centralizada del módulo FM2000.
- Logística y Fletes: Todos los costos de transporte de piezas defectuosas hacia fábrica y el envío de piezas nuevas hacia el sitio serán responsabilidad del contratista.

C. Soporte Técnico y Hardware

- Hardware (RFR): Soporte bajo modalidad de Retorno para Reparación.
- Soporte Remoto: Acceso al Centro de Asistencia Técnica (TAC) del fabricante las 24 horas, los 7 días de la semana.
- Reemplazo de Partes: El contratista gestionará con el fabricante el uso de partes nuevas o equivalentes, para asegurar que el sistema mantenga sus certificaciones y rendimiento original.

D. Limitaciones de Responsabilidad

- El contratista no será responsable por daños causados por **Fuerza Mayor** (desastres naturales comprobables) o actos de vandalismo de terceros, de acuerdo con las exclusiones generales de garantía.
- Toda intervención técnica debe ser realizada por personal certificado para no invalidar el soporte de fábrica.

13.2. Infraestructura de Red – Core y Distribución

- Equipo: Switches Huawei CloudEngine 6866-48S8CQ-P
- Cantidad: 8
- Alcance mínimo:
  - Soporte de hardware con reemplazo avanzado o reparación NBD.
  - Acceso a actualizaciones de software y boletines de seguridad.
  - Soporte técnico especializado de segundo y tercer nivel (TAC).
  - Pruebas de salud semestrales y respaldo de configuraciones.

- Garantía de compatibilidad con trancievers ópticos certificados.

13.2.1. Especificaciones de Soporte y Garantía HI CARE para Switches Tor

El proponente deberá incluir para los ocho (8) switches TOR el paquete de servicios Huawei Hi-Care, asegurando la disponibilidad de expertos técnicos y logística de repuestos bajo las siguientes condiciones:

A. Vigencia y Periodo de Cobertura

- Inicio de la Cobertura: A partir de la suscripción de acta de inicio.
- Duración: Un (1) años (12 meses).
- Disponibilidad: Soporte por suscripción con disponibilidad de expertos 24x7

B. Niveles de Servicio (ANS de Hardware)

- Opción Hi-Care Premier (Crítica): Reemplazo de hardware en un plazo de cuatro (4) horas (24x7x4) para solicitudes de Prioridad 1 y 2.

C. Soporte Técnico Especializado (TAC)

- Acceso 24x7: Consultas técnicas, solución de problemas y solicitudes de servicio a través de líneas directas, correo, web y App móvil (HiKnow).
- Tiempos de Respuesta (TAC): Teniendo en cuenta que los switch TOR corresponden al Cores de conectividad del Datacenter Alterno se requieren tiempos de respuesta para misión crítica.
    - Prioridad 1 (Impacto Crítico): Respuesta en un máximo de 30 minutos.
    - Prioridad 2 (Impacto Alto o Significativo): Respuesta en un máximo de 60 minutos.
    - Prioridad 3 y 4 (Medio y Bajo): Respuesta en 2 horas o al siguiente día hábil respectivamente.

D. Servicios de Atención de Fabricante

- Centro de Mantenimiento Inteligente (ServiceCare): Acceso a la plataforma para gestionar el inventario de los switches por número de serie (SN), visualizar el estado de garantía y generar informes de servicio con un clic.
- Derechos de Actualización de Software: Acceso a actualizaciones del sistema embebido (parches de seguridad, corrección de errores y versiones de mantenimiento) durante toda la vigencia del contrato.
- Auto-ayuda Online: Acceso ilimitado a la comunidad técnica, guías de configuración y al chatbot inteligente "WeiKnow".

E. Responsabilidad del Contratista (Cláusula de Cierre)

- Gestión Integral: El contratista será el responsable de coordinar con Huawei la apertura de casos (SR) y la logística de retorno de partes defectuosas (dentro de los 15 días posteriores al reemplazo).
- Cobertura de Vacíos: Cualquier costo de envío, seguro o soporte en sitio que no sea cubierto por el paquete Hi-Care seleccionado debido a restricciones geográficas (distancia mayor a 50 km de un almacén de repuestos) deberá ser asumido por el contratista.

13.3. ONT Red de Acceso Óptico - GPON

- Equipo: ONT VSOL XPON V2804DAC
- Cantidad: 16
- Alcance mínimo:
  - Reemplazo por falla con equipos nuevos o equivalentes.
  - Soporte de provisión y gestión OMCI / TR-069.
  - Actualización controlada de firmware.
  - Validación de parámetros ópticos y desempeño.
  - Stock de contingencia mínimo del 10%.

13.4. OLT Red de Acceso Óptico - GPON

- Equipo: ONT VSOL GPON V1600GS
- Cantidad: 1
- Alcance mínimo:
  - Cobertura de chasis y módulos ópticos.
  - Acceso a parches y actualizaciones de software.
  - Pruebas periódicas de desempeño GPON.
  - Respaldo de configuraciones y soporte de interoperabilidad.

13.5. Sistema de Detección (Edwards) y Extinción (SEVO Systems) de Incendios y Alarma (Kidde)

El contratista deberá prestar soporte técnico especializado para el Sistema de Detección de Incendios marca Edwards, el Sistema de Extinción mediante agente limpio marca SEVO Systems y el Sistema de Alarma Contra Incendios marca Kidde, actualmente instalados en el Data Center de la Entidad, garantizando su operatividad continua y condiciones óptimas de funcionamiento.

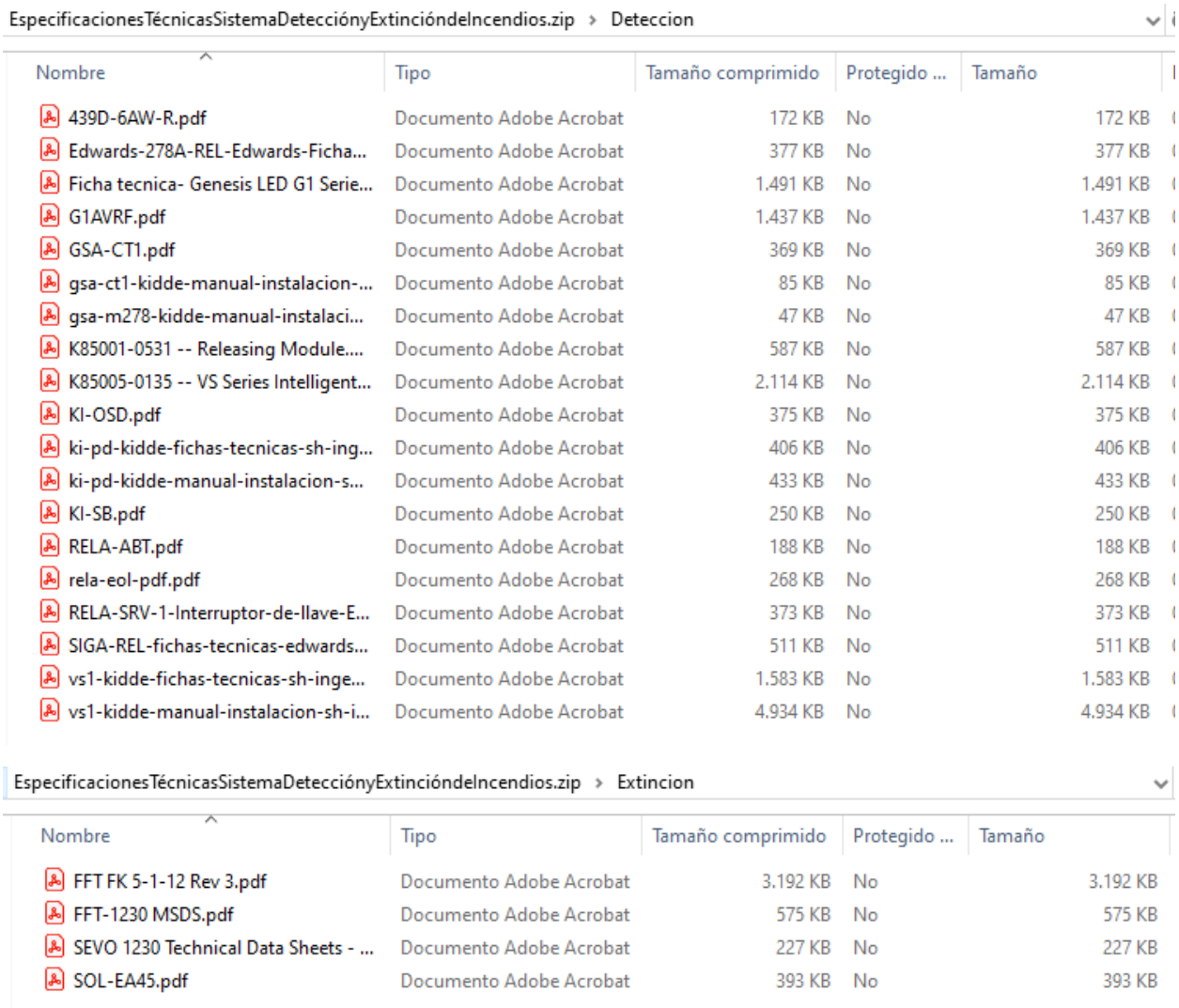
- Cantidad: 1
- Alcance mínimo:
  - Mantenimiento preventivo y correctivo de paneles de control, detectores, módulos, sensores, estaciones manuales y dispositivos asociados.
  - Verificación de la integridad del cableado, lazo de detección y comunicación entre equipos.
  - Pruebas funcionales periódicas conforme a los protocolos técnicos de cada fabricante.
  - Inspección del sistema de extinción SEVO Systems, incluyendo validación del agente limpio, cilindros, válvulas, boquillas y mecanismos de activación.
  - Revisión de baterías de respaldo, fuentes de alimentación y sistemas de notificación audiovisual del sistema Kidde.
  - Actualización de firmware o software cuando aplique y esté autorizado por el fabricante.
  - Emisión de informes técnicos detallados posteriores a cada intervención.
  - Reposición de elementos defectuosos.

La certificación, autorización o aval técnico requerido para este componente puede ser acreditado por el proponente, por cualquiera de los integrantes de una figura plural, o por un aliado/subcontratista especializado formalmente vinculado a la oferta, siempre que se garantice la prestación del mantenimiento preventivo y correctivo, diagnóstico, pruebas funcionales, suministro de repuestos, atención de fallas y soporte especializado sobre dichos sistemas.

Fichas Técnicas e información complementaria

Se adjuntan fichas y documentos con las especificaciones técnicas de Sistema de Detección y Extinción de Incendios en archivo .zip

Nombre del archivo: EspecificacionesTécnicasSistemaDetecciónyExtinciónde Incendios.zip



EspecificacionesTécnicasSistemaDetecciónyExtinciónde Incendios.zip › Deteccion

Nombre	Tipo	Tamaño comprimido	Protegido ...	Tamaño
439D-6AW-R.pdf	Documento Adobe Acrobat	172 KB	No	172 KB
Edwards-278A-REL-Edwards-Ficha...	Documento Adobe Acrobat	377 KB	No	377 KB
Ficha tecnica- Genesis LED G1 Serie...	Documento Adobe Acrobat	1.491 KB	No	1.491 KB
G1AVRF.pdf	Documento Adobe Acrobat	1.437 KB	No	1.437 KB
GSA-CT1.pdf	Documento Adobe Acrobat	369 KB	No	369 KB
gsa-ct1-kidde-manual-instalacion-...	Documento Adobe Acrobat	85 KB	No	85 KB
gsa-m278-kidde-manual-instalaci...	Documento Adobe Acrobat	47 KB	No	47 KB
K85001-0531 -- Releasing Module....	Documento Adobe Acrobat	587 KB	No	587 KB
K85005-0135 -- VS Series Intelligent...	Documento Adobe Acrobat	2.114 KB	No	2.114 KB
KI-OSD.pdf	Documento Adobe Acrobat	375 KB	No	375 KB
ki-pd-kidde-fichas-tecnicas-sh-ing...	Documento Adobe Acrobat	406 KB	No	406 KB
ki-pd-kidde-manual-instalacion-s...	Documento Adobe Acrobat	433 KB	No	433 KB
KI-SB.pdf	Documento Adobe Acrobat	250 KB	No	250 KB
RELA-ABT.pdf	Documento Adobe Acrobat	188 KB	No	188 KB
rela-eol-pdf.pdf	Documento Adobe Acrobat	268 KB	No	268 KB
RELA-SRV-1-Interruptor-de-llave-E...	Documento Adobe Acrobat	373 KB	No	373 KB
SIGA-REL-fichas-tecnicas-edwards...	Documento Adobe Acrobat	511 KB	No	511 KB
vs1-kidde-fichas-tecnicas-sh-inge...	Documento Adobe Acrobat	1.583 KB	No	1.583 KB
vs1-kidde-manual-instalacion-sh-i...	Documento Adobe Acrobat	4.934 KB	No	4.934 KB

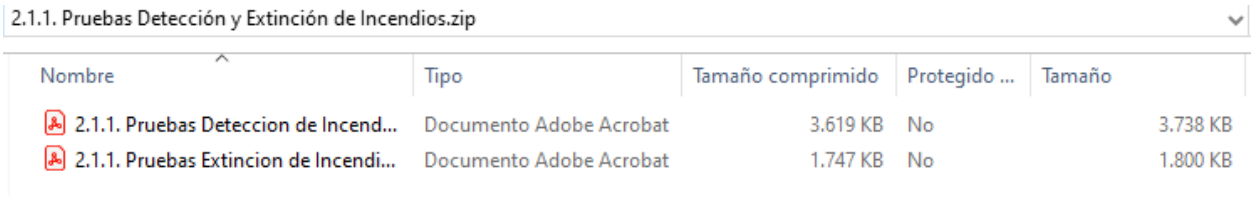
EspecificacionesTécnicasSistemaDetecciónyExtinciónde Incendios.zip › Extincion

Nombre	Tipo	Tamaño comprimido	Protegido ...	Tamaño
FFT FK 5-1-12 Rev 3.pdf	Documento Adobe Acrobat	3.192 KB	No	3.192 KB
FFT-1230 MSDS.pdf	Documento Adobe Acrobat	575 KB	No	575 KB
SEVO 1230 Technical Data Sheets - ...	Documento Adobe Acrobat	227 KB	No	227 KB
SOL-EA45.pdf	Documento Adobe Acrobat	393 KB	No	393 KB

Pruebas de los sistemas de Detección y Extinción de Incendios instalado en el el CTD.

Nombre del archivo: 2.1.1. Pruebas Detección y Extinción de Incendios.zip

Contenido:



Información complementaria.

Fecha de la última recarga Agente Limpio: 18 de diciembre de 2024

Capacidad de los Tanques: 100 Libras y 45 Libras.

El sistema de extención de incendios se integra al Módulo inteligente.

Baterias del panel de control: 18 de diciembre de 2024

Dispositivos conectados a la Alarma: 34.

13.6. Sistema de Respaldo Eléctrico

- Equipo: Planta eléctrica KOHLER J150U_220
- Cantidad: 1
- Alcance mínimo:
  - Revisión y diagnóstico integral de motor, alternador y panel de control.
  - Inspección de motor diésel, sistema de arranque de 24VDC, limpieza de filtros de aire y combustible, y verificación de transferencia automática.
  - Inspección de sistemas de combustible, escape, refrigeración y lubricación
  - Documentación y gestión de la garantía del fabricante
  - Cumplimiento del RETIE y normativa vigente.
  - Pruebas de carga y operación controlada
  - Reemplazo de consumibles y repuestos aprobados por el fabricante
  - Asistencia prioritaria ante fallas o alarmas del sistema
  - Revisión de Potencia: 150 KVA nominal PRIME efectiva a la altitud de Bogotá (2630 msnm).
  - Cumplimiento Normativo: Estándares ISO 8528 para grupos electrógenos y normas de emisión de ruido (Resolución 0627 de 2006).
  - Tableros Eléctricos y PDU: Ajuste de conexiones en el Gabinete de Distribución de Energía (PDC) y monitoreo de las 16 Rack PDU (2 por cada uno de los 8 racks).
  - Puesta a Tierra: Medición de resistividad y estado de varillas/mallas para cumplimiento de norma RETIE.

13.6.1. Especificación del Servicio

El soporte debe ser integral y directo de fábrica para asegurar la continuidad del Datacenter Alterno.

- Disponibilidad: Cobertura total 7x4x365 durante los 12 meses de vigencia.
- Tiempos de Respuesta: Atención de incidentes en un plazo máximo de cuatro (4) horas tras el reporte.
- Reposición de Partes: Reemplazo de componentes defectuosos al siguiente día calendario de la falla.
- Calidad de Repuestos: Todas las partes y piezas deben ser nuevas de fábrica, no remanufacturadas ni reparadas.

13.6.2. Requisitos del Oferente

Para validar la garantía de fábrica, el proveedor debe adjuntar:

- Certificación de Canal: Documento vigente que lo acredite como distribuidor autorizado para comercializar e instalar la marca ofertada.
- Compromiso de Repuestos: Certificación de disponibilidad de partes por un periodo mínimo de cinco (5) años.
- Mesa de Servicio: Software de gestión basado en mejores prácticas ITIL para el registro y seguimiento de casos.
- Actualización de Firmware: El soporte debe incluir la aplicación de parches, fixes y actualizaciones de software de control de forma integrada.

NOTA 1:
Es pertinente precisar que, se autorizan soluciones temporales inmediatas bajo aprobación de la supervisión del contrato, sustentado en garantizar la continuidad de los servicios TIC de la entidad, para lo cual el contratista debe demostrar que se encuentra gestionando la solución definitiva.

NOTA 2: Toda marca o referencia técnica descrita se entiende seguida de la frase "o equivalente", siempre que supere o iguale las condiciones técnicas exigidas.

14. COMPONENTES DE FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DE DATACENTER PRINCIPAL DCP

El contratista deberá realizar el suministro e instalación de siete (7) módulos integrados tipo micro centro de datos "todo en uno" que integre UPS, distribución de energía, refrigeración, monitoreo, baterías y sistema de extinción de incendios dentro de un solo gabinete cerrado, para permitir la instalación en sitio y proteger la infraestructura hiperconvergente de Datacenter Principal con aire acondicionado de precisión y Sistema de detección y extinción de incendios cada módulo integrado debe cumplir las especificaciones técnicas establecidas

14.1. Especificaciones técnicas módulos integrados tipo micro centro de datos

Tabla 7. Especificaciones técnicas módulos integrados tipo micro centro de datos

SUBSISTEMA	ESPECIFICACIÓN REQUERIDA
Gabinete y Estructura	• Dimensiones: 600 mm (Ancho) × 2000 mm (Alto) × 1100/1200 mm (Profundidad) aprox. (Configuración típica de 42U). • Espacio IT Disponible: Mínimo 22U para equipos IT. • Grado de Protección: IP20. • Acceso: El gabinete deberá incluir puerta frontal en vidrio templado de seguridad y puerta posterior sólida o perforada, conforme al diseño de flujo de aire. Asimismo, deberá incorporar sistema de apertura automática de las puertas traseras ante umbrales críticos de temperatura, como medida de protección térmica de los equipos TI.
Sistema de Energía (UPS)	• Capacidad: UPS montada en rack (Rack-mounted). Capacidades disponibles: 3 kVA. • Voltaje de Entrada: 220/230/240 VAC, 1Ph+N+PE, 50/60Hz. • Factor de Potencia: Salida PF = 0.9 o 1.0 • Eficiencia: ≥ 94% en modo normal.
Baterías (Respaldo)	• Tipo: Módulo de baterías de litio tipo SmartLi o equivalentes, integradas e instaladas internamente en el gabinete, diseñadas para respaldo energético de cargas críticas. • Autonomía: Configurable a partir de quince (15) minutos. Cada módulo deberá garantizar una autonomía mínima de quince (15) minutos a plena carga (100% de carga nominal).
Distribución (PDU)	• PDU Integrada: Sistema de distribución eléctrica incorporado en el mismo chasis del UPS o mediante módulo de distribución dedicado, con capacidad de monitoreo y protección de cargas críticas. • Salidas: rPDU vertical u horizontal, con tomas normalizadas tipo IEC C13 y/o IEC C19.
Sistema de Enfriamiento	• Tipo: Unidad de aire acondicionado de precisión tipo In-Rack, instalada dentro del gabinete, con sistema de expansión directa (DX), diseñada para control térmico específico de cargas críticas de TI. • Capacidad de Enfriamiento: 3.5 kW nominales. • Flujo de Aire: El sistema deberá operar con suministro de aire frío por la parte frontal y retorno de aire caliente por la parte posterior del gabinete cerrado, bajo configuración de confinamiento térmico interno (pasillo frío/pasillo caliente), asegurando control ambiental y eficiencia energética. • Refrigerante: R410A.
Gestión y Monitoreo	• Controlador: Módulo ECC800e o similar para gestión centralizada. • Interfaz Local: Pantalla táctil tipo PAD de mínimo diez (10) pulgadas, con capacidad de reconocimiento facial y funcionalidades de gestión y monitoreo visual del sistema. • Acceso Remoto: Plataforma de gestión remota mediante Interfaz WebUI y aplicación móvil, con soporte para protocolos SNMP y Modbus para integración con sistemas de monitoreo y gestión centralizada.
Sensores Incluidos	La unidad debe incluir los siguientes sensores preinstalados: • Sensor de temperatura y humedad. • Sensor de humo. • Sensor de estado de puerta. • Sensor de fugas de agua.
Seguridad Física	• Cerradura: Cerradura electrónica inteligente. • Extinción de Incendios: Módulo de detección y extinción de incendios integrado al rack, con formato 1U o equivalente, que utilice agente limpio tipo perfluorohexanona (FK-5-1-12) o tecnología equivalente certificada, apta para protección de equipos electrónicos y sin generar daño a la infraestructura TI.
Alcance del Suministro	
Cantidad	• siete (7) módulos integrados tipo micro centro de datos (Gabinete, UPS, AA, PDU, Monitoreo).
Baterías	• Cada debe incluir las baterías necesarias para garantizar una autonomía mínima de quince (15) minutos a plena carga (100% de carga nominal).

SUBSISTEMA	ESPECIFICACIÓN REQUERIDA
Entrega	• Entrega en sitio Datacenter Principal y NVC.
Instalación	• Instalación física y eléctrica. Realizar las acometidas desde el tablero principal cumpliendo recomendaciones de fabricante para instalación y garantía de los módulos integrados. • Puesta en marcha (Commissioning) y configuración del sistema de monitoreo local (onsite) y remoto (online). • El sistema debe ser apto para instalación sobre piso de concreto o piso técnico falso.
Condiciones Ambientales	• El equipo debe operar correctamente en un rango de temperatura interior de 0°C a 40°C.
Licenciamiento	• Una licencia de software de gestión de monitoreo local (onsite) y remoto (online) por cada módulo integrado tipo micro centro de datos para la gestión centralizada. Licencias siete (7). • El sistema debe permitir la gestión unificada de las 7 unidades a través de una plataforma gestión centralizada local (onsite) y remoto (online).

15. COMPONENTES FORTALECIMIENTO INFRAESTRUCTURA DE DATACENTER NVC

El contratista deberá realizar el suministro de un servidor para fortalecer los servicios de Protocolo de Configuración Dinámica de Host - DHCP y Directorio Activo - AD en Nivel Central

Realizar la instalación en rack y conectado a fuentes de energía.

La entidad cuenta con Licenciamiento y un equipo de soporte de infraestructura tecnológica con profesionales especializados que realizaran la instalación de Sistema Operativo, Directorio Activo y DHCP.

15.1. Especificaciones técnicas Servidor Datacenter NVC

Tabla 8.

COMPONENTE	ESPECIFICACIÓN TÉCNICA	DETALLE TÉCNICO
Chasis	Rack 1U	El servidor deberá ser de formato rackeable, compatible con gabinetes estándar de 19 pulgadas, e incluir los rieles, soportes y accesorios requeridos para su adecuada instalación en infraestructura de centro de datos.
Procesador (CPU)	Intel Xeon E-2436 (o equivalente).	6 Núcleos / 12 Hilos, 2.9 GHz Base. TDP 65W.
Memoria RAM	64 GB DDR5 ECC UDIMM (4800 MT/s)	La memoria instalada deberá configurarse en dos (2) módulos de treinta y dos (32) GB cada uno, para un total mínimo de sesenta y cuatro (64) GB, en arquitectura Dual Rank,

COMPONENTE	ESPECIFICACIÓN TÉCNICA	DETALLE TÉCNICO
		garantizando óptimo desempeño y balance de canales de memoria. La configuración deberá permitir la disponibilidad de ranuras (slots) libres para futuras ampliaciones, sin requerir el reemplazo de los módulos inicialmente instalados.
Almacenamiento	4 x 960 GB SSD SATA	Los discos deberán configurarse en RAID 1 (espejo) mediante controlador RAID por hardware dedicado, garantizando redundancia y alta disponibilidad de la información. Las unidades de estado sólido (SSD) deberán ser de clasificación empresarial, tipo Read Intensive (RI) o Mixed Use (MU), adecuadas para cargas de trabajo institucionales y operación continua 24/7. El servidor deberá permitir reemplazo de discos en caliente (hot-plug o hot-swap), sin necesidad de apagar el equipo ni interrumpir la operación de los servicios.
Controladora RAID	El servidor deberá incluir controlador RAID por hardware dedicado, integrado de fábrica o mediante tarjeta interna, que no dependa del sistema operativo para la gestión del arreglo de discos. Herramientas de monitoreo e integración con el sistema de gestión remota del servidor. No se aceptarán soluciones de RAID basadas únicamente en software o dependientes del sistema operativo para su funcionamiento.	El controlador deberá cumplir como mínimo con las siguientes características: • Soporte para niveles RAID 0, 1 y 10 . • Gestión autónoma del arreglo de discos, independiente del sistema operativo. • Compatibilidad con discos SSD y/o SAS/SATA según configuración solicitada. • Soporte para discos hot-swap (cambio en caliente). • Funcionalidad de reconstrucción automática del arreglo ante falla de disco. • Memoria caché dedicada
Red (NIC)	Contar como mínimo con dos (2) interfaces de red integradas (onboard) tipo 10/100/1000Base-T, con	Configuración de agregación de enlaces (Link Aggregation) bajo

COMPONENTE	ESPECIFICACIÓN TÉCNICA	DETALLE TÉCNICO
	conector RJ-45, compatibles con cableado estructurado en cobre. Las interfaces deberán ser suficientes para la operación estable y continua de los servicios requeridos, sin afectar el desempeño del servidor. El contratista debe suministrar los cables de red necesarios para la interconexión y puesta en marcha del servidor. Estos deben ser cables categoría 6A F/UTP (o superior) 100% cobre, certificados de fábrica (patch cords), con una longitud mínima de tres (3) metros cada uno, adecuados para el peinado y distribución en los gabinetes del Data Center. El ofrecimiento debe incluir los transceptores multimodo (SFP) compatibles en su totalidad con los switches DELL - HUAWEI - CISCO - FORTINET (10GB).	estándares como IEEE 802.3ad / LACP o equivalente. Implementación de esquemas de redundancia y balanceo de carga (teaming/bonding). Operación adecuada para soportar servicios de infraestructura tales como Directorio Activo (AD), DHCP u otros servicios de red institucionales. La conectividad se realizará hacia el Core o distribución del Data Center de la Entidad mediante enlaces redundantes (LACP/MLAG), garantizando alta disponibilidad en la capa de red
Fuente de Poder	Dual, Hot-Plug Redundant (600W/700W). Debe contar con dos (2) fuentes de poder redundantes (1+1) de instalación en caliente (Hot-Swap) con certificación de eficiencia energética.	Nivel Platinum o Titanium. Crítico para evitar caídas por fallo eléctrico de una fuente.
Gestión Remota	El servidor ofertado deberá contar con módulo de administración remota fuera de banda (out-of-band), integrado de fábrica o mediante licencia avanzada habilitada, que permita la gestión independiente del sistema operativo. El sistema deberá permitir la administración completa del servidor de manera remota, garantizando continuidad operativa, reducción de tiempos de atención y cumplimiento de los niveles de servicio establecidos.	El sistema de gestión remota deberá cumplir como mínimo con las siguientes características: • Acceso remoto seguro vía Web (HTTPS) mediante interfaz gráfica (WebUI). • Consola remota KVM completa (teclado, video y mouse) sin requerir agentes instalados en el sistema operativo. • Encendido, apagado, reinicio y control de energía remoto, incluso cuando el sistema operativo no esté operativo. • Montaje remoto de imágenes ISO o medios virtuales para instalación y recuperación del sistema. • Monitoreo en tiempo real del hardware, incluyendo procesadores, memoria, almacenamiento, ventiladores,

COMPONENTE	ESPECIFICACIÓN TÉCNICA	DETALLE TÉCNICO
		fuentes de poder y sensores de temperatura. • Gestión y descarga de registros de eventos (logs) del sistema. • Soporte para protocolos estándar de integración, tales como SNMP, Redfish, REST API o equivalentes. • Integración con servicios de autenticación centralizada, tales como directorio activo o LDAP. • Puerto de red dedicado para administración remota, independiente de las interfaces de producción. • Licencia avanzada activada, sin requerir costos adicionales durante la vigencia contractual.
Protocolos	El Servidor debe soportar de forma nativa los protocolos IPv4, IPv6, SNMPv3, SSHv2, TLS 1.3 y protocolos de almacenamiento estándar (iSCSI, FC).	Requerido para características de compatibilidad.
Seguridad	Trusted Platform Module - TPM 2.0 definida por el Trusted Computing Group (TCG)	Requerido para características de seguridad de Windows Server (BitLocker, Credential Guard).
Soporte	• Debe soportar una GPU RTX A400 o RTX A1000 • Debe soportar hasta 10 discos de 2.5 pulgadas • Debe soportar PCIe Gen5 • Debe soportar tarjetas LAN 10/25G • **El servidor deberá corresponder a una plataforma empresarial que soporte tecnologías de almacenamiento SAS, SATA y NVMe como parte de su arquitectura y posibilidades de expansión durante su ciclo de vida, mediante componentes, accesorios y kits oficiales del fabricante. No se requiere que la configuración inicialmente ofertada incorpore simultáneamente dichas tecnologías ni que su futura implementación pueda realizarse sin la sustitución o incorporación de componentes propios de la arquitectura del fabricante.**	Los requisitos de capacidad solicitados se constituyen medidas de planeación tecnológica responsable que: Garantizan escalabilidad. Prolongan la vida útil del activo. Evitan reprocesos contractuales. Optimizan el uso eficiente de recursos públicos. Aseguran alineación con la evolución tecnológica del Datacenter Principal y Nivel Central.
Alcance del Suministro		

COMPONENTE	ESPECIFICACIÓN TÉCNICA	DETALLE TÉCNICO
Cantidad	• Un (1) servidor Data Center.	
Entrega	• Entrega en sitio Datacenter NVC.	
Instalación	Instalación física en rack y conexión eléctrica.	
Licenciamiento	• El licenciamiento de sistema operativo y del software DHCP y AD es suministrada por la entidad.	
Configuración	• A cargo de la entidad. Se precisa que la entidad cuenta con persona técnico especializado mediante el Operador Tecnológico contratado para la administración y operación de la infraestructura de Data Center.	
Pruebas de aceptación	• Pruebas de aceptación de usuario (UAT) incluirán pruebas de failover de energía, redundancia de red y validación de rendimiento de lectura/escritura en discos.	

16. PLAN DE MANTENIMIENTO PREVENTIVO PARA INVENTARIO DE ELEMENTOS DE INFRAESTRUCTURA DATA CENTER ALTERNO (TABLA 1.)

Dentro de los treinta (30) días calendario siguientes a la suscripción del Acta de Inicio, el contratista deberá presentar para aprobación de la supervisión un Plan de Trabajo de Mantenimiento Preventivo para la infraestructura tecnológica objeto del presente proceso.

El contratista está obligado a ejecutar al menos dos (2) mantenimientos preventivos anuales, separados con mínimo 4 meses entre el primer y segundo mantenimiento.

Dicho plan deberá incluir como mínimo:

- Repaso y validación detallada del alcance del servicio.
- Identificación y análisis de riesgos asociados a la operación y mantenimiento.
- Definición de planes de contingencia y procedimientos de atención ante incidentes.
- Cronograma de actividades de mantenimiento preventivo.
- Designación de responsables técnicos.
- Relación de puntos de contacto y canales de escalamiento.

El plan deberá estar alineado con los requisitos establecidos en el anexo técnico y garantizar la continuidad operativa de la infraestructura tecnológica.

16.1. Guía de especificación de plan de mantenimiento

La especificación del plan de mantenimiento a manera ilustrativa se presenta en el numeral anterior como guía, no obstante, el contratista está obligado a entregar un plan detallado ajustado con su criterio técnico y recomendaciones de cada fabricante.

1) Preparación y seguridad (1 hora)

Actividades

- Reunión de apertura: repaso de alcance, riesgos, planes de contingencia, responsables y puntos de contacto.
- Verificación de permisos: trabajo en alturas (si aplica), procedimiento de seguridad en intervenciones eléctricas y revisión el mecanismo de comunicaciones ante incidentes.
- Respaldo y congelamiento: confirmación de respaldos de configuración de red y estado de alarmas.

Entregables: Acta de inicio, matriz de riesgos, plan de trabajo del día.

2) Sistema modular de Data Center – FM2000 (1,5 horas)

Objetivo: garantizar operación estable del módulo, sensores y eficiencia energética.

Actividades

- Inspección visual y mecánica: puertas, paneles, sellos, bandejas, cableado estructurado y orden.
- Limpieza de filtros y revisión de obstrucciones en flujos de aire; verificación de PUE y tendencias del último cuatrimestre.
- Pruebas de sensores y alarmas (temperatura, humedad, humo), chequeo del sistema de monitoreo y eventos.
- Validación de versiones y, si procede, actualización de firmware y controladores.

Criterios de aceptación: sin alarmas latentes, PUE dentro de umbrales definidos, registros en BMS actualizados.

Entregables: checklists firmados, fotos de filtros, log de eventos.

Módulos exteriores de enfriamiento – NetCol500 (1,5 horas)

Objetivo: asegurar la gestión térmica y estabilidad de los racks.

Actividades

- Inspección de unidades exteriores: ventiladores, vibraciones, soportes y conexiones.
- Verificación de parámetros térmicos y flujo de aire; ajuste fino si es necesario.
- Pruebas de eficiencia energética (consumo vs. carga térmica) y revisión de controladores, sensores y alarmas específicas.

- Limpieza liviana (externa) y programación de limpieza profunda si se evidencia suciedad crítica.

Criterios de aceptación: capacidad térmica disponible ≥ demanda pico estimada; sin alarmas; estabilidad.

Entregables: captura de tendencias, reporte de calibración y fotografías de estado.

Pausa operativa / almuerzo (1 hora)

- Revisión de avances vs. plan; confirmación de no afectación de servicios.

3) Red – Core y distribución (CE6866-48S8CQ-P) (13:00–14:30)

Objetivo: salud de hardware, estabilidad de software y respaldo de configuraciones.

Actividades

- Pruebas de salud: temperatura, PSU, ventiladores, errores en puertos, ópticos críticos.
- Respaldo de configuraciones y verificación de integridad; comparación con baseline.
- Revisión de boletines de seguridad y disponibilidad de actualizaciones de software; plan de ventana si se requiere.
- Validación de compatibilidad con transceivers ópticos certificados y niveles de potencia.

Criterios de aceptación: sin flaps, redundancia operativa OK.

Evidencia: outputs de salud.

4) Red de acceso óptico – GPO N (1 hora)

Objetivo: asegurar desempeño estable del acceso óptico.

Actividades

- OLT VSOL V1600GS: revisión de chasis/módulos, logs, óptica PON, estado de servicios.
- ONT VSOL V2804DAC (muestra representativa): verificación OMCI/TR 069, niveles ópticos y firmware.
- Validación de stock de contingencia y reemplazo por falla.

Criterios de aceptación: potencias en rango, cero alarmas críticas, servicios levantados.

Entregables: reporte de niveles ópticos, lista de ONT muestreadas, plan de actualización si aplica.

5) Respaldo eléctrico – Planta KOHLER J150U_220 (1 hora)

Objetivo: confiabilidad del suministro y cumplimiento normativo.

Actividades

- Inspección general: combustible, lubricación, refrigeración, batería de inicio, interruptor de transferencia.
- Pruebas funcionales sin carga y verificación de alarmas.
- Verificación de cumplimiento y registros de mantenimiento.

Criterios de aceptación: arranque dentro de tiempos esperados, parámetros eléctricos en rango, sin fugas/ruidos anómalos.

Entregables: Hoja de ruta de pruebas, curvas de carga, registro fotográfico.

6) Detección y extinción de incendios – Sistema KIDDE (1 hora)

Objetivo: asegurar operatividad de detección y accionamiento conforme a normas aplicables.

Actividades

- Pruebas funcionales (muestrales o 100% según plan anual) de detectores, estaciones manuales, sirenas.
- Verificación de integridad de agentes/medios de extinción, presiones y fecha de recarga.
- Revisión de eventos históricos.

Criterios de aceptación: tiempos de respuesta dentro de lo esperado, restablecimiento correcto, cero dispositivos fuera de servicio.

Entregables: Actas de prueba y certificación alineada con NFPA 72 o normas técnicas aplicables.

7) Cierre y entrega (0,5 horas)

- Restitución de condiciones y verificación final de alarmas = 0.
- Acta de cierre, hallazgos clasificados (críticos/altos/medios/bajos), plan de acciones con responsables y fechas.
- Entrega de paquete de evidencias: checklists, respaldos de configuración, reportes de tendencias térmicas/eléctricas, fotografías, bitácora de incidentes y recomendaciones de mejora continua.

Roles mínimos

- Coordinador de mantenimiento (punto de control, seguridad y tiempos).
- Especialista HVAC (FM2000).

- Ingeniero de redes (core/distribución y GPON).
- Técnico eléctrico (planta y tableros).
- Técnico de seguridad contra incendios (detección/acción).

17. CERTIFICACIÓN DE LA CASA MATRIZ, AUTORIZACIÓN DE SERVICIOS

Por cada uno de los componentes de infraestructura incluidos en el presente proceso, la Secretaría de Educación del Distrito requiere que los proponentes alleguen la acreditación a través de **una (1) certificación expedida por el fabricante o por el representante de la marca en Colombia**, donde indique que el proponente está autorizado para prestar los servicios de soporte técnico con suministro de partes.

La certificación debe estar dirigida a la Secretaría de Educación del Distrito y debe ser expedida con máximo 30 días calendario de antelación a la fecha de presentación de ofertas.

En caso de que la documentación sea presentada por un proponente plural, el requisito se entenderá cumplido cuando alguno de los integrantes presente la certificación en los términos aquí solicitados

17.1. Certificación de fabricante requerida – Soporte Módulo inteligente FM2000

El proponente deberá acreditar certificación vigente expedida directamente por el fabricante Huawei, que lo habilite para prestar servicios de soporte técnico especializado sobre el Módulo Inteligente de Data Center, bajo la denominación:

- Huawei Data Center Facility 3Star CSP (Certified Service Partner).

Dicha certificación deberá:

- Estar vigente a la fecha de cierre de presentación de ofertas y durante la ejecución contractual, el contratista estará obligado a mantener la vigencia de sus competencias técnicas, permitiéndose la acreditación de su renovación o continuidad formalizada ante el fabricante una vez se cumplan las ventanas de tiempo internas dispuestas por Huawei para tal fin. El Proponente podrá acreditar la condición Huawei Data Center Facility 3Star CSP – Certified Service Partner mediante certificación física, constancia o validación oficial del fabricante Huawei, incluyendo sus portales o mecanismos oficiales de consulta.

  En caso de que la certificación alcance su fecha de vencimiento durante la ejecución contractual, el contratista deberá acreditar la renovación, conforme a los procedimientos y cronogramas del fabricante, garantizando en todo momento que el mantenimiento sea ejecutado por personal autorizado, condición indispensable para mantener la vigencia de la garantía de los equipos.

- Acreditar de manera expresa la competencia técnica del proponente para realizar actividades de soporte, diagnóstico, mantenimiento y atención de incidentes sobre la solución indicada.

- Ser presentada en idioma español o inglés; en caso de idioma diferente, deberá anexarse la traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.
- La no presentación de esta certificación, o su presentación sin vigencia o sin correspondencia directa con la denominación requerida, dará lugar a la no habilitación del proponente en el componente técnico.

17.2. Certificación de fabricante requerida – Soporte Especializado Switches Huawei

El proponente deberá acreditar certificación vigente expedida directamente por el fabricante Huawei, que lo acredite como Huawei Partner Gold, para la prestación de servicios de soporte técnico especializado sobre switches marca Huawei y módulo inteligente.

La certificación deberá cumplir con las siguientes condiciones:

- Estar vigente al momento del cierre del proceso y durante la ejecución del contrato.
- Acreditar la condición de partner autorizado en categoría Gold, con facultades para comercialización, soporte, implementación y mantenimiento de soluciones de networking Huawei.
- Ser expedida directamente por el fabricante o consultable mediante portal oficial del fabricante.
- En caso de estar en idioma diferente al español, deberá adjuntarse traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La no acreditación de esta certificación en los términos exigidos dará lugar a la no habilitación técnica del proponente, por tratarse de un requisito que garantiza la idoneidad, respaldo del fabricante y continuidad del soporte sobre la infraestructura crítica de la entidad.

17.3. Certificación de fabricante requerida – Soporte Planta Eléctrica

El proponente deberá acreditar certificación vigente expedida directamente por el fabricante **Kohler**, que lo autorice para prestar servicios de soporte técnico especializado y mantenimiento a la planta eléctrica instalada en la entidad o que el servicio será prestado directamente por el fabricante a través de sus canales autorizados.

La certificación deberá cumplir, como mínimo, con las siguientes condiciones:

- Estar vigente al momento del cierre del proceso de selección y mantenerse durante toda la ejecución del contrato.
- Acreditar de manera expresa que el proponente se encuentra autorizado por el fabricante para realizar actividades de mantenimiento preventivo y correctivo, diagnóstico, pruebas de carga,

configuración, suministro e instalación de repuestos originales y atención de emergencias sobre la planta eléctrica objeto del contrato.

- Garantizar acceso a soporte técnico especializado del fabricante cuando se requiera, así como el uso de repuestos y componentes originales que preserven las condiciones de garantía y operación segura del equipo.
- Ser expedida directamente por el fabricante o ser verificable a través de sus canales oficiales.
- En caso de encontrarse en idioma diferente al español, deberá adjuntarse la respectiva traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La exigencia de esta certificación tiene como finalidad garantizar la idoneidad técnica del contratista, la continuidad operativa del sistema de respaldo eléctrico, la preservación de la garantía del fabricante y el cumplimiento de la normativa aplicable en materia de seguridad eléctrica y protección de infraestructura crítica de la entidad.

La no acreditación de este requisito en los términos establecidos dará lugar a la no habilitación técnica del proponente.

17.4. Certificación de fabricante requerida – Sistema de Detección de Incendios

El proponente podrá presentar cualquiera de las siguientes alternativas:

- **Certificación vigente expedida por el fabricante, mediante la cual se autorice al proponente, al fabricante o a sus canales de servicio oficialmente autorizados para prestar los servicios de soporte técnico especializado y mantenimiento de los sistemas instalados; o**
- **Certificaciones, constancias o comprobantes vigentes de capacitación, entrenamiento o autorización del personal técnico que ejecutará las actividades de soporte y mantenimiento, expedidos por los fabricantes Edwards, SEVO Systems o Kidde, o por sus centros de entrenamiento oficialmente autorizados, que acrediten su formación y competencia técnica para intervenir los equipos objeto del contrato.**

La certificación deberá:

- Estar vigente al momento del cierre y presentación de ofertas del proceso de selección y mantenerse durante toda la ejecución contractual.
- Acreditar que el proponente está autorizado para prestar soporte y mantenimiento al Sistema de Detección de incendios por el fabricante para intervenir la solución.
- Ser expedida directamente por el fabricante
- En caso de estar en idioma diferente al español, deberá anexarse la traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La exigencia de esta certificación se establece con el fin de garantizar la idoneidad técnica del contratista, la continuidad operativa del sistema de protección contra incendios y la preservación de las condiciones de garantía y cumplimiento normativo aplicable.

La no acreditación en los términos señalados dará lugar a la no habilitación técnica del proponente.

17.5. Certificación de fabricante requerida – Sistema de Extinción de Incendios

El proponente podrá presentar cualquiera de las siguientes alternativas:

- **Certificación vigente expedida por el fabricante, mediante la cual se autorice al proponente, al fabricante o a sus canales de servicio oficialmente autorizados para prestar los servicios de soporte técnico especializado y mantenimiento de los sistemas instalados; o**
- **Certificaciones, constancias o comprobantes vigentes de capacitación, entrenamiento o autorización del personal técnico que ejecutará las actividades de soporte y mantenimiento, expedidos por los fabricantes Edwards, SEVO Systems o Kidde, o por sus centros de entrenamiento oficialmente autorizados, que acrediten su formación y competencia técnica para intervenir los equipos objeto del contrato.**

La certificación deberá cumplir con las siguientes condiciones:

- Estar vigente al momento del cierre del proceso y mantenerse durante la ejecución contractual.
- Acreditar que el proponente es autorizado para prestar soporte y mantenimiento al Sistema de Extinción de incendios por el fabricante para intervenir la solución.
- Ser expedida directamente por el fabricante
- En caso de estar en idioma diferente al español, deberá adjuntarse la traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La exigencia de esta certificación tiene como finalidad asegurar la idoneidad técnica del contratista, la continuidad operativa del sistema de protección contra incendios y el cumplimiento de la normatividad aplicable en materia de seguridad física y protección de infraestructura crítica.

La no acreditación de este requisito en los términos señalados dará lugar a la no habilitación técnica del proponente.

17.6. Certificación de fabricante requerida – Sistemas Inteligentes de Alarma contra Incendios

El proponente podrá presentar cualquiera de las siguientes alternativas:

- **Certificación vigente expedida por el fabricante, mediante la cual se autorice al proponente, al fabricante o a sus canales de servicio oficialmente autorizados para prestar los servicios de soporte técnico especializado y mantenimiento de los sistemas instalados; o**
- **Certificaciones, constancias o comprobantes vigentes de capacitación, entrenamiento o autorización del personal técnico que ejecutará las actividades de soporte y mantenimiento, expedidos por los fabricantes Edwards, SEVO Systems o Kidde, o por sus centros de entrenamiento oficialmente autorizados, que acrediten su formación y competencia técnica para intervenir los equipos objeto del contrato.**

La certificación deberá cumplir, como mínimo, con las siguientes condiciones:

- Estar vigente al momento del cierre del proceso de selección y mantenerse durante toda la ejecución contractual.
- Acreditar que el proponente está autorizado por el fabricante para prestar soporte y mantenimiento a los Sistemas Inteligentes de Alarma contra Incendios instalados en la entidad.
- Ser expedida directamente por el fabricante .
- En caso de estar en idioma diferente al español, deberá adjuntarse la respectiva traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La exigencia de esta certificación tiene como finalidad garantizar la idoneidad técnica del contratista, la correcta operación y continuidad del sistema de protección contra incendios, la preservación de las condiciones de garantía del fabricante y el cumplimiento de la normativa aplicable en materia de seguridad física y protección de infraestructura crítica de la entidad.

La no acreditación de este requisito en los términos señalados dará lugar a la no habilitación técnica del proponente.

17.7. Certificación de fabricante requerida – Módulo integrado tipo micro centro de datos

El proponente deberá acreditar certificación vigente expedida directamente por el fabricante del Módulo integrado tipo micro centro de datos, que lo acredite como Partner de alguno de los dos niveles más altos de membresía, para el suministro, instalación y soporte de la prestación de servicios de soporte técnico especializado del módulo integrado tipo micro centro de datos.

- La certificación deberá cumplir con las siguientes condiciones:
- Estar vigente al momento del cierre del proceso y durante la ejecución del contrato.
- Acreditar la condición de partner autorizado en categoría de alguno de los dos niveles más altos de membresía, con facultades para comercialización, soporte, implementación y mantenimiento del módulo integrado tipo micro centro de datos.
- Ser expedida directamente por el fabricante o consultable mediante portal oficial del fabricante.

- En caso de estar en idioma diferente al español, deberá adjuntarse traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La no acreditación de esta certificación en los términos exigidos dará lugar a la no habilitación técnica del proponente, por tratarse de un requisito que garantiza la idoneidad, respaldo del fabricante y continuidad del soporte sobre la infraestructura crítica de la entidad.

17.8. Certificación de fabricante requerida – Servidor para Data Center

El proponente deberá acreditar certificación vigente expedida directamente por el fabricante que lo acredite como distribuidor autorizado o canal oficial para el suministro, instalación y la prestación de servicios de soporte técnico especializado del SERVIDOR.

- Debe ser presentada junto con la oferta y estar vigente al momento del cierre del proceso y durante la ejecución del contrato.
- La certificación debe ser consultable mediante el portal oficial del fabricante.
- En caso de estar en idioma diferente al español, deberá adjuntarse traducción simple al castellano, bajo la responsabilidad y firma del representante legal del proponente.

La no acreditación de esta certificación en los términos exigidos dará lugar a la no habilitación técnica del proponente, por tratarse de un requisito que garantiza la idoneidad, respaldo del fabricante y continuidad del soporte sobre la infraestructura crítica de la entidad.

18. ACUERDOS DE NIVELES DE SERVICIO (ANS)

Modelo de horas de servicio compensado por vencimiento de los plazos contractuales pactados en ANS.

18.1. Horas de Servicio por Compensación (Bolsa de Horas por Demanda)

Con el propósito de compensar los incumplimientos en los tiempos de respuesta, entrega, instalación o configuración definidos en los Acuerdos de Niveles de Servicio (ANS), el contratista deberá constituir una bolsa de Horas de Servicio Especializado, las cuales serán ejecutadas bajo demanda de la SED durante la vigencia de la garantía (un año).

18.2. Naturaleza de las Horas de Servicio

Las Horas de Servicio corresponden al tiempo técnico especializado adicional, sin costo para la SED, orientado a fortalecer, optimizar o asegurar la operación de la infraestructura tecnológica del Data Center, y se generan por incumplimientos en los ANS definidos en el contrato a manera de compensación.

Estas horas:

- No constituyen pago en dinero ni reconocimiento económico.
- No son acumulables como saldo financiero.
- Son exigibles por la SED en cualquier momento dentro de la vigencia contractual.

18.3. Características del Servicio

Las horas deberán ser prestadas bajo las siguientes condiciones:

- Modalidad: Remota y/o presencial según la necesidad.
- Cobertura: Aplicable sobre la totalidad de la infraestructura objeto del contrato (DCA, DCP y NVC).
- Perfil del recurso: Personal técnico certificado o autorizado por fabricante, de acuerdo con lo exigido en el Anexo Técnico.
- Disponibilidad: Coordinada con la SED, sin afectar la operación (ventanas programadas o atención controlada).

18.4. Tipología de Actividades Ejecutables

Las Horas de Servicio podrán ser utilizadas por la SED para la ejecución de actividades como:

- Diagnóstico avanzado y análisis de causa raíz (RCA) de incidentes.
- Afinamiento (tuning) de configuraciones de infraestructura (red, energía, climatización, GPON, etc.).
- Actualización controlada de firmware, software o parches de seguridad.
- Revisión de arquitectura y recomendaciones de mejora.
- Ejecución de mantenimientos adicionales no programados.
- Pruebas de resiliencia, continuidad y recuperación (DRP).
- Optimización de desempeño (performance tuning).
- Acompañamiento técnico en cambios mayores o ventanas críticas.
- Transferencia de conocimiento al equipo técnico de la SED.

18.5. Activación y Gestión

- La SED solicitará la ejecución de las horas mediante requerimiento formal al contratista.
- El contratista deberá presentar un plan de trabajo específico por cada solicitud.
- Cada ejecución deberá generar:
- Informe técnico detallado
- Registro de horas consumidas
- Resultados obtenidos y recomendaciones

18.6. Control y Trazabilidad

El contratista deberá llevar un control detallado de:

- Horas generadas por incumplimientos
- Horas ejecutadas
- Saldo disponible

Este control deberá ser reportado en los informes de soporte.

18.7. Vigencia

Las Horas de Servicio:

- Podrán ser utilizadas exclusivamente durante el periodo de garantía (12 meses).
- No podrán trasladarse a vigencias futuras.
- Se perderán si no son utilizadas dentro del plazo contractual.

18.8. Descripción de ANS por línea de servicio

18.8.1. Renovación de soporte y garantía de la infraestructura tecnológica de Data Center alterno DCA

Tabla 9 – Nivel de severidad de casos de servicio

Componente	Nivel de Severidad	
FM2000	1	Crítica
CloudEngine 6866-8S8CQ-P	2	Alta
XPON V2804DAC	2	Alta
GPON OLT V1600GS	2	Alta
Sistema de detección y extinción de incendios	1	Crítica
Planta eléctrica J150U_220	2	Alta

Tabla 10 - ANS: Compensación en horas de servicio por incumplir el tiempo estimado de respuesta

Nivel de Severidad	Denominación	Cobertura Horaria	Tiempo Estimado de Respuesta	Tiempo real de atención	Compensación horas Servicio
1	Crítica	24x7	Hasta 2 horas	Mayor a 2 horas	1 hora de servicio por cada 2 horas de retraso
2	Alta	24x7	Hasta 4 horas	Mayor a 4 horas	1 hora de servicio por cada 4 horas de retraso
3	Media	Horario laboral estándar	Hasta 12 horas	Mayor a 12 horas	1 hora de servicio por cada 12 horas de retraso
Nota: el tiempo de respuesta y atención inicia a partir del registro del caso en la plataforma de servicio dispuesta por el contratista.					

18.8.2. Suministro e implementación de los componentes para Data Centers DCP y NVC

Tabla 11 - ANS: Compensación en horas de servicio por incumplir el tiempo de entrega o el tiempo de instalación o configuración.

Hito	Por cada semana de atraso respecto a la fecha inicialmente acordada en el cronograma del proyecto
Para la entrega física de los equipos.	2 horas de compensación por cada semana de atraso
Para la configuración e instalación de los equipos.	1 horas de compensación por cada semana de atraso

19. ACUERDOS DE CONFIDENCIALIDAD

Toda información obtenida por el CONTRATISTA así como sus informes y documentos que produzca, relacionados con la ejecución del contrato, son considerados confidenciales, por lo que el CONTRATISTA no

podrá divulgarlos sin autorización expresa por escrito de la SED, en ese sentido, el CONTRATISTA debe aceptar y firmar los acuerdos de confidencialidad de la información, los cuales deben hacerse explícitos desde el momento de la operación y estar firmados para permitir el acceso a la información o servicios de procesamiento de información de la SED.

GLOSARIO

Arquitectura Hiperconvergente: La infraestructura hiperconvergente (HCI) es un sistema unificado y definido por software que reúne todos los elementos de un centro de datos tradicional: almacenamiento, recursos informáticos, red y gestión

Arquitectura onpremise: "On-premises" significa en español "en las instalaciones propias" o "in situ". Esta definición de on-premises se refiere a la utilización de servidores y entorno informático propios de la empresa. Cuando se recurre a este modelo de utilización, el cliente alquila, en calidad de titular de la licencia, un software basado en servidor que se instala en un servidor propio o alquilado.

Bypass Externo: Equipo de protección para permitir o no el paso de energía normal o regulada. El modo Bypass significa que el UPS proporciona la energía directamente sin ningún tipo de regulación, si el controlador detecta que la red es anormal, se apagara la salida para proteger la carga.

Data Center: "Datacenter" Se denomina Centro de Proceso de Datos al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

GPON: Tecnología de acceso de telecomunicaciones que utiliza fibra óptica, la Red Óptica Pasiva con Capacidad de Gigabit (GPON o Gigabit-capable Passive Optical Network en inglés)

Infraestructura Hiperconvergente: infraestructura de información que integra recursos y dispositivos informáticos virtuales, combinando el almacenamiento, la computación y la conectividad de la red en un solo chasis o nodo, con el fin de reducir la complejidad de los centros de datos y facilitar la escalabilidad. Agrega una capa de software de virtualización que permite la administración de la totalidad de recursos en un nodo o clúster.

Nube: "Cloud" La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o simplemente «la nube», es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es internet.

Onpremise: Infraestructura o servicios instalados en el sitio propio de la organización o entidad.

PDU: Los PDU para racks están diseñados para distribuir energía a todos los tipos de equipos de TI dentro del centro de datos. Las unidades de distribución de energía para racks (PDU para racks) son el último eslabón de la cadena energética y garantizan la entrega de energía esencial para las cargas de TI.

SFP: Transceptor SFP o Mini-GBIC, del inglés small form-factor pluggable transceiver (en español transceptor enchufable de pequeña forma) o, también en inglés, SFP transceptor y de forma abreviada conocido como SFP o Mini-GBIC, es un transceptor compacto y conectable en caliente utilizado para las aplicaciones de comunicaciones de datos y telecomunicaciones. Están diseñados para soportar Sonet, canal de Fibra, Gigabit Ethernet y otros estándares de comunicaciones.

TOR: “Switch TOR” ToR (Top of Rack) es una forma común de enrutamiento de servidor a switch o de switch a switch. El switch ToR puede ser un switch de capa de acceso, un switch de capa de agregación o un switch de capa central. Cuando el switch ToR está ubicado en la parte superior del gabinete del servidor y cumple la función de conectar el servidor y el switch de la capa central o de la capa de agregación, se denomina switch de la capa de acceso. Cuando el switch ToR está ubicado en la parte superior del switch gabinete, se llama capa de agregación o switch de capa central.

Tabla 12. AUTORES ANEXO TÉCNICO

ROL	NOMBRE
Elaboró Aspectos Técnicos	Omar Ardila Torres. - Profesional Contratista OTIC Jairo Alberto Orduz Salamanca – Profesional Especializado OTIC
Revisó Aspectos Jurídicos	Helbert Alfonso Suárez Gómez – Profesional Contratista OTIC
Revisó Aspectos Técnicos	Carlos Alberto López Díaz – Profesional Contratista OTIC
	Jorge Iván Vergara Sornoza – Profesional Contratista OTIC