DATASET

SERVICIOS ESPECIALIZADOS EN TELECOMUNICACIONES DATASET S.A.S.
NIT 901.106.067-8
CR 42B 88-59
Tel: (035) 3860408
Barranquilla - Colombia
asistente1@datasetsas.com

Factura electrónica de venta
No. FE 689

Señores	E.S.E HOSPITAL LOCAL DE CARTAGENA DE INDIAS-		
NIT	806.010.305-8	**Teléfono**	(000) 0000000
Dirección	*Pie de la popa, calle Nueva del Toril. Calle 33 #22-54*	**Ciudad**	Cartagena - Colombia

Fecha y hora Factura

Generación	06/03/2026, 09:55
Expedición	06/03/2026, 10:24
Vencimiento	21/03/2026

Ítem	Descripción	Cantidad	Vr. Total
1	INTERNET DEDICADO TECNOLOGÍA TERRESTRE(FO.RE). INTERNET SATELITAL. CIBER-SEGURIDAD SOPHOS. SERVIDOR CENTRAL DEDICADO + INTERCONEXION EN LA NUBE. A55 1.8 GHZ	1.00	141,607,025.00

Hospital Local Cartagena de Indias

RECIBIDO PARA SU ESTUDIO Y PÚBLICA ACEPTACIÓN

14 ABR 2026

SF - 1311

No. Radicado:

Recibido: Oriana 3:19 pm

Total items: 1

Total Bruto	118,997,500.00
IVA 19%	22,609,525.00
Total a Pagar	141,607,025.00

Valor en Letras:
Ciento cuarenta y un millones seiscientos siete mil veinticinco pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Otro - Clientes Nacionales - Cuota No. 001 vence el 2026-03-21 por $ 141,607,025.00

Observaciones:
Periodo: 01 al 28 de febrero de 2026
Fecha limite de pago : 21 de marzo de 2026
Nota. consignar a la cuenta de ahorros Bancolombia N°55483509871 a nombre de Servicios Especializados en Telecomunicaciones Dataset S.A.S

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764092957717 aprobado en 20250508 prefijo FE desde el número 501 al 1000 Vigencia: 12 Meses**
Responsable de IVA - Actividad Económica 6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas Tarifa 0.96%
CUFE: 372b5d7d5412ff3418165e6a0ba6bb2e308ef304589eb368e45467007aa48e5909ccc9ec870430dbacc60024b4ec0340

Fabricante Software y Proveedor tecnológico: Siigo SAS - Nit 830.048.145-8. Nombre Software: Siigo Nube. Firma electrónica: ver en el XML

Código: FTO-GAJ-SCAP-22
Versión: 4
Fecha: 26/02/2025

FORMATO DE SUPERVISION DE CONTRATOS Y AUTORIZACION DE PAGOS

Dependencia:	SISTEMAS	Número de pago/ total de pagos:	1/1	Fecha:	13/04/2026

DATOS DEL CONTRATO

Valor:	$ 141.607.025,00			Valor mensual	$ 141.607.025,00 $ 0,00
Número:	050-26	Fec.Suscripción	5/02/2026	Fecha de Iniciación:	cinco (05) de Febrero de 2026
Nº CDP 1:	0589	Fecha:	29/01/2026	Fecha de terminación:	cuatro (04) de Marzo de 2026
Nº CDP 2:		Fecha:			
Nº RP 1:	0609	Fecha:	30/01/2026	Duración:	1 Meses
Nº RP 2:		Fecha:		Periodo a pagar:	FEBRERO
Rubro Presupuestal:	245020883161			Suspensión No.:	En tiempo:
Requiere Informe:	SI: X		NO:	Prorroga No.:	En tiempo:
Entregó Informe:	SI: X		NO:		

OBJETO DEL CONTRATO: SERVICIOS DE CONECTIVIDAD DE INTERNET DEDICADO, CIBERSEGURIDAD Y SERVICIOS CLOUD PUBLICA, QUE PERMITA CONECTAR LA TOTALIDAD DE LAS SEDES QUE CONFORMAN LA ESE HOSPITAL LOCAL DE CARTAGENA.

INFORMACIÓN BÁSICA DEL CONTRATISTA

Nombre:	DATASET S.A.S NIT 901106067-8								
Identificación:	Tipo de documento: Cédula		NIT	X	Número:	901.106.067	DV.	8	
Dirección:	CR 51 B 86 PLAZA 51 LC 9						CEL.	3016145657	
Número de Teléfono:	3214510400		FAX:				Banco:	Bancolombia	
Clase y número de cuenta:	Corriente:		Ahorros	X	Número	55483509871			

ASPECTOS TRIBUTARIOS

Marque con "X"				
Persona Natural:		Persona Jurídica:	X	
Gran Contribuyente:		Autoretenedor:		
Responsable de IVA	X	Entidad sin ánimo de lucro		
NO responsable de IVA				
He verificado de esta información frente al RUT :			SI: X	NO:

INFORME DEL SUPERVISOR

El contratista presentó el informe correspondiente:	SI: X	NO:	# de folios:	
El informe cumple con lo estipulado en el contrato:	SI: X	NO:		

AVANCE DEL CONTRATO POR ACTIVIDAD

Observaciones del supervisor a las actividades ejecutadas:

Se anexa informe de supervision de ejecucion contractual (FTO-SAF-ISEC) e Informe de actividades realizados por el contratista

APORTES SEGURIDAD SOCIAL

Persona Natural:

Aportes a Salud			Aportes a Pensión		
Valor pagado $	Periodo	mar-26	Valor pagado $	Periodo	feb-26
Comprobante de pago Número:		9500750345	Comprobante de pago Número Planilla:		9500750345
Fecha de pago:		2 de marzo de 2026	Fecha de pago:		2 de marzo de 2026

Aportes a A.R.L.		
Valor pagado $	Periodo	
Comprobante de pago Número:		9500750345
Fecha de pago:		2 de marzo de 2026

Persistencia:	SI:	NO:
Certificación:	SI:	NO:
	SI:	NO:

Persona Jurídica:

SOLICITUD DE PAGO

Certifico que las actividades se están ejecutando conforme a lo establecido en el contrato, que el contratista cumplió con los pagos de seguridad social en salud, pensión y Administradora de Riesgos Laborales conforme a las normas vigentes, por lo tanto autorizo el pago de la factura FE689 por valor de $ 141.607.025,00

Anexos:						
Copia de aporte a pensión	SI: X	NO:	Cuenta de Cobro	SI:	NO:	
Copia de aporte a salud	SI: X	NO:	factura	SI: X	NO:	FE689
Copia de aporte A.R.L.	SI: X					

FIRMA CONTRATISTA

NOMBRE CONTRATISTA: ANDRES FELIPE CASAS CASTELLANOS

C.C.: 1.098.662.851 DE BUCARAMANGA

DENOMINACIÓN DEL CARGO: REPRESENTANTE LEGAL

DATASET S.A.S

Yeinis Palomino E

FIRMA SUPERVISOR

NOMBRE SUPERVISOR: YEINIS PALOMINO ESTRADA

C.C.: 1050719449 DE MAGANGUE

DENOMINACION DEL CARGO: DIRECTORA OFICINA TECNOLOGIAS DE LA INFORMACIÓN

AREA ASIGNADA: OFICINA DE TECNOLOGIAS DE LA INFORMACION

NOMBRE APOYO SUPERVISION

CARGO:

Hospital Local Cartagena	INFORME DE ACTIVIDADES CONTRATISTAS	Código: FTO-SAF-INCO-28 Versión: 1 Fecha: 07/07/2020

CONTRATO N° 050-26

NOMBRE DEL CONTRATISTA: DATASET S.A.S NIT: 901106067-8

IDENTIFICACION: 901106067-8

FECHA DE INICIO	05 DE FEBRERO DE 2026
PERIODO DEL INFORME	FEBRERO
LUGAR DE EJECUCION (area)	SEDE ADMINISTRATIVA Y CENTROS DE SALUD ESE HLCI

OBJETO DEL CONTRATO

SERVICIO DE CONECTIVIDAD DE INTERNET DEDICADO, CIBERSEGURIDAD Y SERVICIO CLOUD PUBLICA, QUE PERMITA CONECTAR LA TOTALIDAD DE LAS SEDES QUE CONFORMAN LA ESE HOSPITAL LOCAL DE CARTAGENA.

ACTIVIDADES REALIZADAS EN EL PERIODO DE ACUERDO CON LAS OBLIGACIONES ESPECIFICAS ESTABLECIDAS EN EL CONTRATO

OBLIGACIONES	DESCRIPCION DE LOS SOPORTES DE ACTIVIDADES DESARROLLADAS
1, Garantizar el ancho de banda establecido a cada sede de la ESE HOSPITAL LOCAL DE CARTAGENA.	Se realizó monitoreo continuo del consumo de ancho de banda en cada sede mediante herramientas especializadas (PRTG Network Monitor), evidenciando el cumplimiento del 100% de la capacidad contratada. De esta herramienta se compartió un link de monitoreo a la entidad contratante, con la información que se relaciona a continuación: https://200.7.110.29:443 Usuario: Soporte Contraseña: k478H&V&H$ Donde la entidad, a través del personal de la mesa de ayuda y soporte técnico podía supervisar el cumplimiento de los ANS de disponibilidad y ancho de banda por cada uno de los centros de salud conectados. De igual manera, hace parte integral del presente documento el Informe de Gestión Mensual del periodo contratado, donde se relaciona las actividades de reporte de cambios que afecten la topología de la red, cambio de equipos; Reporte de Mantenimientos Programados, Reporte de la Gestión de la Mesa de Ayuda con la documentación de los tickets sobre las incidencias reportadas durante el periodo; y finalmente el reporte de las actividades de Ciberseguridad.
2. Presentar un cronograma de Instalación a las diferentes sedes de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS de los canales dedicados.	Teniendo en cuenta que el presente contrato corresponde a una segunda prorroga/adición al contrato previamente ejecutado (Contrato de Prestación de Servicios No. 093-25) (Prorroga/adición #1 Orden de Servicios No. 005-26), bajo los mismos términos técnicos y operativos, se precisa que la infraestructura de conectividad y los canales dedicados en las diferentes sedes de la ESE Hospital Local Cartagena de Indias ya se encuentran instalados y en operación desde la fase inicial del contrato. En este sentido, no se requiere un cronograma de instalación desde cero, sino un cronograma de verificación, validación y continuidad del servicio, orientado a garantizar que las condiciones contratadas se mantengan durante el periodo de la adición.

3. Brindar Soporte de Asistencia técnica.	El cumplimiento de la presente obligación se encuentra debidamente soportado mediante la elaboración y entrega del informe mensual de gestión de actividades, en el cual se consolidan de manera detallada los hitos del proyecto y las actividades ejecutadas durante el periodo evaluado. Dicho informe incluye: La descripción de las actividades técnicas realizadas, orientadas a garantizar la operación continua de los servicios de conectividad. El seguimiento a los hitos del proyecto, evidenciando el avance y cumplimiento de las obligaciones contractuales. La relación de tickets gestionados a través de la mesa de ayuda, incluyendo: Número de caso Fecha de apertura y cierre Tipo de incidente o requerimiento Tiempo de atención y solución Estado (cerrado/en proceso) El registro de incidentes y acciones correctivas, donde se detallan las actividades de diagnóstico, atención y solución implementadas. El reporte de actividades de ciberseguridad, incluyendo las medidas de mitigación aplicadas frente a eventos detectados, tales como: Gestión de vulnerabilidades Aplicación de parches y actualizaciones Monitoreo de tráfico y eventos de seguridad Contención de incidentes y acciones preventivas En conjunto, esta información permite evidenciar de manera integral la prestación continua del servicio de soporte técnico, garantizando la atención oportuna de incidentes, la estabilidad de la infraestructura tecnológica y la implementación de buenas prácticas en materia de seguridad de la información.
4. Analítica de la red y sus aplicaciones.	El cumplimiento de esta obligación se soporta mediante la implementación de procesos de monitoreo, análisis y evaluación continua del desempeño de la red y de las aplicaciones que operan sobre la misma, cuyos resultados se consolidan en el informe mensual de gestión.Se incluye: Herramienta de Monitoreo de red, que permite analizar el comportamiento del tráfico en cada una de las sedes, incluyendo consumo de ancho de banda, picos de utilización y patrones de uso. Indicadores de desempeño (KPIs), tales como: Disponibilidad del servicio (% uptime) Latencia Pérdida de paquetes Uso promedio y máximo del canal Posibles congestiones o degradaciones del servicio Identificación de eventos y anomalías, tales como: Saturación de enlaces Comportamientos inusuales de tráfico Posibles incidentes de seguridad Acciones de mejora implementadas, incluyendo: Optimización del tráfico Priorización de aplicaciones (QoS) Ajustes en configuración de red Lo anterior permite garantizar una gestión proactiva de la red, orientada a la mejora continua del servicio y al aseguramiento del correcto funcionamiento de las aplicaciones institucionales.

5. Máximo aprovechamiento de los recursos de red.	El cumplimiento de esta obligación se soporta mediante la implementación de estrategias de optimización, control y monitoreo de los recursos de red, orientadas a garantizar un uso eficiente del ancho de banda y de la infraestructura tecnológica disponible. Lo anterior con el desarrollo continuo de las siguientes actividades: Monitoreo continuo del uso del ancho de banda, identificando patrones de consumo y posibles subutilizaciones o saturaciones en las diferentes sedes. Implementación de políticas de priorización de tráfico (QoS), garantizando el correcto funcionamiento de las aplicaciones críticas institucionales frente a otros tipos de tráfico no prioritario. Optimización de la configuración de red, incluyendo ajustes en equipos activos (routers, switches, firewalls) para mejorar el rendimiento y la estabilidad del servicio. Estas acciones permiten garantizar el uso racional y eficiente de los recursos de red, asegurando la continuidad operativa y el adecuado desempeño de los servicios tecnológicos en todas las sedes.
6. Eficiencia en los servicios de red altamente críticos	El cumplimiento de esta obligación se soporta en la garantía de disponibilidad, desempeño y continuidad de los servicios de red considerados críticos para la operación de la entidad. En este sentido, se precisa que el objetivo principal de la infraestructura de conectividad es asegurar la interconexión de las diferentes sedes con los servicios centralizados, tanto en la sede principal como en la nube pública, donde se encuentran alojadas las plataformas institucionales. Es por ello, que el cumplimiento de las actividades anteriormente mencionadas garantiza la eficiencia de estos servicios, debidamente soportados en la gestión realizada a través de la mesa de ayuda y soporte técnico.
7. Integración con Nubes (Privada, Pública e híbrida).	Se precisa que el componente de integración con servicios de nube (privada, pública e híbrida) fue implementado durante la ejecución del contrato inicial No. 093-25, en el cual se establecieron los mecanismos de interconexión entre las sedes de la entidad, la infraestructura centralizada y los servicios alojados en la nube. En el marco de la presente adición contractual, las actividades desarrolladas se han orientado a garantizar la continuidad, estabilidad y eficiencia de dicha integración, la cual constituye el punto neurálgico de la operación de la entidad, al soportar el acceso a los sistemas de información institucionales.
8. Servicio de interconexión, que garantice la comunicación constante entre la sede administrativa y los centros de salud.	El cumplimiento de esta obligación se soporta en la garantía de conectividad permanente entre la sede administrativa y los diferentes centros de salud, permitiendo el acceso continuo a los servicios institucionales alojados en los servidores centrales y en la nube pública. Durante el periodo evaluado, se evidencia la disponibilidad del servicio de interconexión, reflejada en la ausencia de reportes de indisponibilidad total que hayan impedido el acceso a los sistemas institucionales por parte de las sedes. Así mismo, en los casos en los que se presentaron incidencias parciales o degradaciones del servicio, estas fueron: Reportadas a través de la mesa de ayuda Atendidas oportunamente por el equipo técnico Gestionadas hasta su solución Documentadas en el informe de gestión Adicionalmente, se realiza monitoreo continuo de la conectividad, verificando parámetros como disponibilidad, latencia y estabilidad de los enlaces, lo cual permite garantizar la comunicación constante entre las sedes y la correcta operación de los servicios institucionales. En conjunto, estas acciones evidencian el cumplimiento de la obligación, asegurando la interconectividad efectiva entre la sede administrativa y los centros de salud.

9. Mantenimientos preventivos y correctivos a las torres y mástiles.	n relación con la presente obligación, se precisa que la infraestructura implementada durante la ejecución del contrato inicial No. 093-25 no contempló el uso de torres ni mástiles para la prestación del servicio de conectividad. Lo anterior, en razón a que la solución tecnológica adoptada se basa en el uso de canales dedicados y/o infraestructura de red soportada en medios cableados como la fibra óptica, radioenlaces y/o enlaces satelitales provistos por el operador, sin requerir estructuras de soporte tipo torres o mástiles. En consecuencia, durante la ejecución del presente contrato y su adición, no se hace aplicable la realización de mantenimientos preventivos o correctivos sobre este tipo de infraestructura, al no existir dichos elementos dentro del alcance técnico del servicio contratado. No obstante, se garantiza el mantenimiento y correcto funcionamiento de los demás componentes de la infraestructura de red implementada, los cuales son atendidos conforme a los procedimientos establecidos y se encuentran debidamente soportado en el informe mensual de gestión
10. Instalación y puesta en marcha de la Ciberseguridad.	Se precisa que la implementación de los componentes de ciberseguridad fue realizada durante la ejecución del contrato inicial No. 093-25, en el cual se efectuó la instalación, configuración y puesta en marcha de los mecanismos de protección de la infraestructura tecnológica de la entidad. En el marco de las adiciones contractuales, las actividades desarrolladas se han orientado a garantizar la continuidad operativa, actualización y fortalecimiento de los controles de ciberseguridad implementados, asegurando la protección de la red y de los servicios institucionales. En este sentido, aunque la instalación inicial fue ejecutada en el contrato base, la presente ejecución contractual garantiza la operación continua, actualización y efectividad de los mecanismos de ciberseguridad, evidenciando su cumplimiento a través de los reportes mensuales de gestión.
11. Presentar un cronograma de Implementación de la ciberseguridad el cual integre los 48 canales dedicados de las diferentes sedes de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS y el servicio Cloud Publica.	Se precisa que la implementación inicial de la arquitectura de ciberseguridad, incluyendo la integración de los canales dedicados y los servicios en la nube pública, fue ejecutada en el marco del contrato de prestación de servicios No. 093-25. En el contexto de la presente adición contractual, las actividades se han orientado a garantizar la continuidad operativa, validación, monitoreo y fortalecimiento de los controles de ciberseguridad, abarcando los 48 canales dedicados de las diferentes sedes y su integración con los servicios en la nube pública.
12. Soporte para incidentes.	El cumplimiento de esta obligación se garantiza mediante la operación de una mesa de ayuda , a través de la cual se gestionan de manera centralizada los incidentes y requerimientos reportados por las diferentes sedes. Los incidentes son atendidos conforme a procedimientos establecidos, los cuales incluyen: Recepción y registro del incidente, asignando un número de ticket para su trazabilidad. Clasificación y priorización, de acuerdo con el impacto y criticidad del evento. Diagnóstico y atención, por parte del equipo técnico especializado. Resolución y cierre, garantizando la restauración del servicio. Seguimiento, en caso de requerirse acciones adicionales. Así mismo, todos los incidentes gestionados son documentados y consolidados en los informes mensuales de gestión, donde se detalla: Relación de tickets atendidos Tipo de incidente Tiempos de respuesta y solución Acciones implementadas Estado de cierre En conjunto, estas acciones evidencian la correcta prestación del servicio de soporte, asegurando la continuidad operativa de la red y de los servicios asociados.

13. Soporte Técnico	El cumplimiento de esta obligación se garantiza mediante la atención integral de requerimientos e incidentes a través de la mesa de ayuda, complementada con la disponibilidad de personal técnico calificado para atención en sitio, cuando las condiciones del evento así lo requieren. Conforme a los registros de tickets gestionados, en aquellos casos donde no fue posible la solución remota, se realizó el desplazamiento de personal técnico a las sedes afectadas, asegurando una atención oportuna y eficiente. Las actividades de soporte técnico incluyen: Diagnóstico de fallas en infraestructura de red y equipos asociados Intervención técnica en sitio para la solución de incidentes Restablecimiento del servicio en el menor tiempo posible Validación de la operación posterior a la atención Todas las actuaciones se encuentran debidamente documentadas en los tickets de la mesa de ayuda, donde se registra:
14. Monitoreo de Infraestructura de prestación de servicios de Ciber Seguridad.	El cumplimiento de esta obligación se soporta mediante el uso de herramientas especializadas de monitoreo, a través de las cuales se supervisa de manera continua la infraestructura de ciberseguridad implementada. En este sentido, el operador dispone de un dashboard de monitoreo, desde el cual se gestionan y visualizan los eventos de seguridad, permitiendo el seguimiento en tiempo real del comportamiento de la red y de los mecanismos de protección. A partir de esta plataforma, se desarrollan las siguientes actividades: Monitoreo continuo de eventos de seguridad, identificando amenazas, accesos no autorizados y comportamientos anómalos. Generación de alertas tempranas, que permiten una respuesta oportuna ante incidentes. Análisis de logs y registros de seguridad, para la detección de posibles vulnerabilidades o riesgos. Seguimiento a indicadores de seguridad, tales como número de eventos, incidentes detectados y mitigados, y niveles de riesgo.
15. Generación de reportes de los incidentes de seguridad encontrados con entrega de reportes semanales /quincenales /mensuales.	El cumplimiento de esta obligación se soporta mediante la generación periódica de reportes de incidentes de seguridad, los cuales son elaborados a partir del monitoreo continuo de la infraestructura tecnológica y de los eventos detectados en la red. En este sentido, los reportes de incidentes de seguridad se encuentran consolidados en el documento denominado "Reporte de Actividades de Ciberseguridad", el cual hace parte integral del informe mensual de gestión presentado por el operador.
16. Aplicación de cambios en políticas de seguridad.	El cumplimiento de esta obligación se soporta mediante la gestión y aplicación controlada de cambios en las políticas de seguridad de la infraestructura tecnológica, en respuesta a requerimientos operativos y necesidades de las diferentes sedes. En este sentido, a través de la mesa de ayuda se reciben solicitudes relacionadas con ajustes en las políticas de seguridad, tales como la habilitación o restricción de accesos a sitios web, aplicaciones o servicios específicos. Particularmente, se evidencian casos en los cuales las sedes han solicitado la habilitación de URLs que inicialmente fueron bloqueadas por los sistemas de ciberseguridad, al ser clasificadas como potencialmente no seguras. Estas solicitudes son: Registradas mediante tickets, garantizando su trazabilidad Evaluadas por el equipo técnico, validando su pertinencia y nivel de riesgo Aprobadas y aplicadas de manera controlada, en caso de ser procedente Documentadas en los informes mensuales de gestión En este sentido, se evidencia el cumplimiento de la obligación mediante los registros de tickets, las configuraciones aplicadas y su respectiva documentación en los informes mensuales de gestión.

17. Gestión de respaldos de configuración	El cumplimiento de esta obligación se soporta en la implementación y operación de mecanismos de respaldo y sincronización de la información y configuraciones críticas de la infraestructura tecnológica. En el marco del contrato de prestación de servicios No. 093-25, se estableció un esquema de sincronización permanente entre los servidores ubicados en la sede principal y los servicios en la nube pública, garantizando la disponibilidad y resguardo de la información ante posibles fallas o eventos que afecten la operación. Durante la ejecución de la presente adición contractual, se ha dado continuidad a esta estrategia mediante: Verificación periódica de los procesos de respaldo y sincronización, asegurando su correcta ejecución. Monitoreo de la integridad y disponibilidad de la información respaldada. Validación de la recuperación de configuraciones, en caso de requerirse restablecimiento de servicios. Actualización de respaldos, conforme a los cambios realizados en la infraestructura y configuraciones de red. Estas actividades permiten garantizar la protección de las configuraciones críticas, así como la continuidad operativa de los servicios tecnológicos de la entidad. Así mismo, se precisa que los respaldos generados se encuentran disponibles para la entidad en el momento en que sean requeridos, garantizando el acceso oportuno a la información y configuraciones necesarias para procesos de verificación, auditoría o recuperación. En este sentido, se da cumplimiento a la obligación contractual, asegurando la adecuada gestión de respaldos, su disponibilidad y la continuidad de la operación ante escenarios de contingencia.
18. Implementación de la suscripción nueva a la Cloud Publica.	Se precisa que la implementación de la suscripción a servicios de nube pública fue realizada en el marco del contrato de prestación de servicios No. 093-25, en el cual se efectuó la configuración, puesta en marcha e integración de los servicios cloud con la infraestructura tecnológica de la entidad. Durante la ejecución de la presente adición contractual, se ha dado cumplimiento a esta obligación mediante la continuidad operativa, administración y aprovechamiento de la suscripción a la nube pública, garantizando la disponibilidad de los servicios institucionales alojados en dicho entorno. En este sentido, se han desarrollado las siguientes actividades: Administración de la suscripción cloud, asegurando su correcto funcionamiento y disponibilidad. Monitoreo de los servicios en la nube, verificando desempeño, acceso y estabilidad. Integración continua con las sedes y canales dedicados, garantizando el acceso a los sistemas institucionales. Gestión de incidentes asociados a la nube, atendidos y documentados a través de la mesa de ayuda. Seguimiento al uso de recursos en la nube, asegurando su adecuado aprovechamiento. Los resultados de estas actividades se encuentran documentados en los informes mensuales de gestión, donde se evidencia la operación continua de la nube pública, su integración con la infraestructura de red y su aporte a la prestación de los servicios institucionales. En este sentido, se da cumplimiento a la obligación contractual, garantizando la disponibilidad, operación y correcta gestión de la suscripción a la nube pública.
19. Instalación y arranque instancia/servicio, configuración S.O. lanzamiento de las instancias de acuerdo con la necesidad de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS.	Se precisa que la instalación, configuración y puesta en marcha de las instancias y servicios en la nube pública, incluyendo la configuración de los sistemas operativos, fue ejecutada durante la fase inicial del contrato de prestación de servicios No. 093-25, conforme a las necesidades operativas de la ESE Hospital Local Cartagena de Indias. En el marco de la presente adición contractual, el operador ha garantizado la continuidad operativa, administración y disponibilidad de dichas instancias, asegurando su correcto funcionamiento y alineación con los requerimientos de la entidad. Para ello, se han desarrollado las siguientes actividades: Administración de instancias en la nube, garantizando su disponibilidad y desempeño. Monitoreo continuo de los servicios desplegados, verificando su estabilidad y correcto funcionamiento. Gestión de configuraciones del sistema operativo, incluyendo actualizaciones, ajustes y optimización. Aprovisionamiento o ajuste de instancias, de acuerdo con nuevas necesidades o requerimientos de la entidad. Gestión de incidentes asociados a los servicios, atendidos y documentados a través de la mesa de ayuda. Estas actividades permiten garantizar la operatividad continua de los servicios desplegados en la nube, así como su adaptación a las necesidades cambiantes de la entidad. Los soportes correspondientes se encuentran documentados en los informes mensuales de gestión, donde se evidencian las actividades realizadas, el estado de las instancias y las acciones de administración ejecutadas. En este sentido, se da cumplimiento a la obligación contractual, asegurando la disponibilidad, administración y adecuado funcionamiento de las instancias y servicios implementados.

20. Despliegue de Bases de Datos: Creación de la base de datos, creación de la replicación	Se precisa que la creación, configuración y puesta en marcha de las bases de datos, así como la implementación de los mecanismos de replicación, fue realizada en el marco del contrato de prestación de servicios No. 093-25, conforme a los requerimientos operativos de la ESE Hospital Local Cartagena de Indias. En este contexto, la replicación de las bases de datos se constituye como el motor principal de la prestación del servicio, al garantizar la disponibilidad, integridad y continuidad de la información crítica de la entidad. Durante la ejecución de la presente adición contractual, el operador ha dado cumplimiento a esta obligación mediante la administración, monitoreo y verificación continua de los procesos de replicación, asegurando el correcto funcionamiento de las bases de datos en los diferentes entornos (sede principal y nube pública). Estas acciones permiten asegurar la disponibilidad permanente de la información, así como la continuidad operativa de los servicios institucionales que dependen de las bases de datos. En este sentido, se da cumplimiento a la obligación contractual, garantizando el correcto despliegue, replicación y operación continua de las bases de datos como componente esencial del servicio.
21. Configuración de los Servicios de Almacenamiento en la Nube	Se precisa que la configuración e implementación de los servicios de almacenamiento en la nube fue realizada en el marco del contrato de prestación de servicios No. 093-25, en el cual se establecieron los mecanismos de almacenamiento, gestión y disponibilidad de la información institucional en entornos cloud. Durante la ejecución de la presente adición contractual, se ha dado cumplimiento a esta obligación mediante la continuidad operativa, administración y monitoreo de los servicios de almacenamiento en la nube, garantizando la disponibilidad, integridad y seguridad de la información. Todas las acciones adelantadas permiten garantizar la disponibilidad permanente de la información, así como su protección y acceso oportuno por parte de los usuarios autorizados. Así mismo, se precisa que toda la información almacenada, de propiedad de la entidad, se encuentra amparada bajo el principio de confidencialidad, garantizando su protección frente a accesos no autorizados, y se encuentra disponible para la entidad en el momento en que sea requerida, asegurando su acceso oportuno para fines operativos, administrativos o de auditoría. En este sentido, se da cumplimiento a la obligación contractual, asegurando la correcta configuración, operación, seguridad y disponibilidad de los servicios de almacenamiento en la nube.

22. Configuración de los Servicios de Conectividad en la Nube.	Se precisa que la configuración de los servicios de conectividad en la nube fue implementada durante la ejecución del contrato de prestación de servicios No. 093-25, en el cual se establecieron los mecanismos de interconexión entre las sedes de la entidad, la infraestructura centralizada y los servicios alojados en la nube pública. En el marco de la presente adición contractual, se ha dado cumplimiento a esta obligación mediante la continuidad operativa, monitoreo y optimización de los servicios de conectividad en la nube, garantizando el acceso permanente y seguro a los sistemas institucionales. Se han implementado acciones que permiten garantizar la comunicación constante, segura y eficiente entre la infraestructura local y los servicios en la nube, soportando la operación de los sistemas institucionales. Los soportes correspondientes se encuentran documentados en los informes mensuales de gestión, donde se evidencian las actividades realizadas, el estado de la conectividad y las acciones implementadas. En este sentido, se da cumplimiento a la obligación contractual, asegurando la correcta configuración, operación y disponibilidad de los servicios de conectividad en la nube.
23.Configuración de los Servicios de Seguridad en la Nube: Configurar listas de control de acceso, grupos de seguridad, configuración de las llaves, solicitud de certificados iniciales, instalación de certificados	Se precisa que la configuración de los servicios de seguridad en la nube fue implementada desde la suscripción del contrato de prestación de servicios No. 093-25, en el cual se establecieron los mecanismos de protección, control de accesos y aseguramiento de la información en los entornos cloud. En el marco de la presente adición contractual, se ha dado cumplimiento a esta obligación mediante la continuidad operativa, administración y monitoreo de los servicios de seguridad en la nube, garantizando la protección de los recursos, aplicaciones y datos institucionales.
24. Configuración de soluciones de respaldo: Creación de políticas y planes de respaldo, configuración y replicación de los archivos.	Se precisa que la creación de las políticas, planes de respaldo y la configuración de los mecanismos de replicación de la información fueron implementadas desde el génesis del contrato de prestación de servicios No. 093-25, en el cual se definieron los lineamientos para la protección, disponibilidad y recuperación de la información institucional. En el marco de la presente adición contractual, se ha dado cumplimiento a esta obligación mediante la continuidad operativa, ejecución, monitoreo y verificación de las soluciones de respaldo, garantizando la protección de los datos y la recuperación oportuna ante eventuales fallas. Así mismo, se precisa que la información respaldada se encuentra disponible para la entidad en el momento en que sea requerida, asegurando su acceso oportuno para procesos operativos, administrativos o de contingencia.
25. Soporte técnico	Durante la ejecución del contrato de prestación de servicios No. 093-25 y su presente adición, no se han presentado incidentes que hayan requerido intervenciones correctivas mayores en los servicios en la nube. No obstante, el operador ha dado cumplimiento a esta obligación mediante la disponibilidad permanente de personal técnico especializado, garantizando la atención oportuna de cualquier eventualidad y la continuidad de los servicios. En este sentido, se han dispuesto las siguientes acciones: Disponibilidad de personal profesional capacitado, con competencias en infraestructura cloud, conectividad y ciberseguridad. Soporte preventivo y acompañamiento técnico, orientado a evitar la materialización de incidentes. Capacidad de respuesta ante eventos no previstos, asegurando tiempos de atención acordes a los niveles de servicio establecidos. Articulación con la mesa de ayuda, para la gestión y escalamiento de requerimientos en caso de ser necesario. Estas acciones han permitido mantener la operatividad continua de los servicios en la nube, sin afectaciones que comprometan la prestación del servicio. En este sentido, se da cumplimiento a la obligación contractual, garantizando la disponibilidad de soporte técnico especializado para atender de manera oportuna cualquier requerimiento de la entidad

FIRMA DEL CONTRATISTA: _____ **NOMBRE DEL CONTRATISTA:** DATASET S.A.S **IDENTIFICACION:** NIT 901106067-8 **REPRESENTANTE LEGAL:** ANDRES FELIPE CASAS CASTELLANOS **CC :** 1.098.662.851 DE BUCARAMANGA	**FIRMA DEL SUPERVISOR:** Yeinis Palomino E **NOMBRE DEL SUPERVISOR:** YEINIS PALOMINO ESTRADA **CARGO DEL SUPERVISOR:** JEFE DE OFICINA TIC

Hospital Local Cartagena	INFORME SUPERVISION DE EJECUCION CONTRACTUAL	Código: FTO-SAF- ISEC-28 Versión: 1 Fecha: 07/07/2020

NO. CONTRATO: 050-26	
NOMBRE DEL CONTRATISTA: DATASET S.A.S NIT: 901106067-8	
IDENTIFICACION: 901106067-8	
FECHA DE INICIO	05 DE FEBRERO DE 2026
PERIODO DEL INFORME	ENERO
LUGAR DE EJECUCION (area)	SEDE ADMINISTRATIVA Y CENTROS DE SALUD ESE HLCI

OBJETO DEL CONTRATO

SERVICIO DE CONECTIVIDAD DE INTERNET DEDICADO, CIBERSEGURIDAD Y SERVICIO CLOUD PUBLICA, QUE PERMITA C ECTAR LA TOTALIDAD DE LAS SEDES QUE CONFORMAN LA ESE HOSPITAL LOCAL DE CARTAGENA,

ACTIVIDADES REALIZADAS EN EL PERIODO DE ACUERDO CON LAS OBLIGACIONES ESPECIFICAS ESTABLECIDAS EN EL CONTRATO

OBLIGACIONES	ACTIVIDADES EJECUTADAS PARA LA VERIFICACION DEL CUMPLIMIENTO DE LA OBLIGACION	RESULTADO CUMPLE/NO CUMPLE
1, Garantizar el ancho de banda establecido a cada sede de la ESE HOSPITAL LOCAL DE CARTAGENA.	El contratista garantizó el ancho de banda contratado en cada sede de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS	CUMPLE
2. Presentar un cronograma nstalación a las diferentes sedes de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS de los canales dedicados.	El contratista presentó cronograma de mantenimiento preventivo a los canales dedicados de datos de las diferentes sedes de la ESE HLCI	CUMPLE
3. Brindar Soporte de Asistencia técnica.	El contratista brindó soporte tecnico a tiempos de respuesta y solución	CUMPLE
4. Analítica de la red y sus aplicaciones.	El contratista presenta informes mensual de gestión que incluye herramienta para el monitoreo de la red	CUMPLE

5. Máximo aprovechamiento de los recursos de red.	El contratista garantiza el máximo aprovechamiento de los recursos de red esto mediante monitoreo, implementación de políticas, optimizacion de configuración de red.	CUMPLE
6. Eficiencia en los servicios de red altamente críticos	El contratista asegura eficiencia en los servicios de red altamente críticos en la ESE HLCI Como en la nube pública.	CUMPLE
7. Integración con Nubes (Privada, Pública e híbrida).	durante la ejecucióm del contrato se mantiene la integración de red servidores destinados para las aplicaiones	CUMPLE
8. Servicio de interconexión, que garantice la comunicación constante entre la sede administrativa y los centros de salud.	El contratista garantiza la conectividad entre las sedes, realiza purebas de comunicación entre la sede administrativa y los centros de salud, permitiendo el acceso a los servicios institucionales.	CUMPLE
9. Mantenimientos preventivos y correctivos a las torres y mástiles.		NO APLICA
10. Instalación y puesta en marcha de la Ciberseguridad.	El contratista inplementa y configura las soluciones de ciberseguridad requeridas	CUMPLE
11. Presentar un cronograma de Implementación de la ciberseguridad el cual integre los 48 canales dedicados de las diferentes sedes de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS y el servicio Cloud Publica.	El contratista ejecutó enla implementación inicial de la qrquitectura de ciberseguridad la integración de los canales dedicados de datos de las diferentes sedes de la ESE HLCI, dando conectidad en el periodo del presente contrato	CUMPLE
12. Soporte para incidentes.	El contratista reporta y brinda soporte ante cualquier registro de incidentes	CUMPLE
13. Soporte Técnico	El contratista brinda soporte tecnico ante cualquier reporte de las sedes	CUMPLE

4. Monitoreo de nfraestructura de prestación e servicios de Ciber eguridad.	El contratista implementa monitoreo continuo de eventos de Ciberseguridad, identificando amenazas, accesos no autorizados y comportamientos anómalos.	CUMPLE
5. Generación de reportes e los incidentes de eguridad encontrados con ntrega e reportes semanales quincenales /mensuales.	El contratista aporta informes mensuales de incidentes de seguridad	CUMPLE
6. Aplicación de cambios en olíticas de seguridad.	El contratista informa sobre la aplicación de cambios en politicas de seguridad	CUMPLE
7. Gestión de respaldos de onfiguración	El contratista gestiona respaldos de configuración en la nube	CUMPLE
8. Implementación de la uscripción nueva a la Cloud ublica.	El contratista implementó suscripción a la nueva Cloud Publica mediante contrato N° 093-25 en el cual se llevó a cabo el proceso de configuración.	CUMPLE
9. Instalación y arranque nstancia/servicio, onfiguración S.O. anzamiento de las nstancias de acuerdo con la ecesidad de la ESE IOSPITAL LOCAL CARTAGENA DE INDIAS.	El contratista realiza instalación, configuración y puesta en marcha de nuevas instancias de acuerdo a las necesidades de la ESE HOSPITAL LOCAL CARTAGENA DE INDIAS durante la fase inicial del contrato N° 093-25	CUMPLE
0 Despliegue de Bases de [illegible]: Creación de la base e datos, creación de la eplicación	El contratista llevó a cabo el despliegue de creación de base de datos y replicación mediante contrato N° 093-25 conforme a los requqrimientos de la ESE HLCI	CUMPLE
1. Configuración de los ervicios de Almacenamiento n la Nube	El contratista realizó configuración de servicios de almacenamiento en la nube el el marco del contrato N° 093-25	CUMPLE
2. Configuración de los ervicios de Conectividad en a Nube.	El contratista realizó configuraración de servicios de conectividad en la nube en el cual se establecieron los mecanismos de interconexión entre las sedes de la ESE HLCI.	CUMPLE

23.Configuración de los Servicios de Seguridad en la Nube: Configurar listas de control de acceso, grupos de seguridad, configuración de las llaves, solicitud de certificados iniciales, instalación de certificados.	El contratista configuró servicios de seguridad en la nube como *Listas de control de acceso *Grupos de seguridad *Llaves de acceso *Certificados digitales, los cuales fueron implementados durante el contrato N° 093-25. Se mantuvieron durante en contrato N° 050-26 las políticas anteriormente mencionadas para el periodo del presente contrato	CUMPLE
24.Configuración de soluciones de respaldo: creación de politicas y planes de respaldo, configuración y replicación de los archivos.	El contratista implementó la creación de políticas, planes de respaldo y configuraciones mediante contrato N° 093-25, dando continuidad a la misma en el periodo del presente contrato	CUMPLE
25. Soporte técnico	El contratista brinda soporte técnico a la infraestructura implementada, atiende incidentes de conectividad y seguridad, escalando incidentes críticos cuando sea necesario	CUMPLE
Observaciones:		

NOMBRE: YEINIS PALOMINO ESTRADA
FIRMA DEL SUPERVISOR

CARGO: DIRECTORA OFICINA TEGNOLOGIAS DE LA INFORMACIÓN

Certificación
Bancaria

Febrero 27 de 2026

Señores:
A QUIEN INTERESE

BANCOLOMBIA S.A. se permite informar que la empresa **SERVICIOS ESPECIALIZADOS EN TELECOMUNICACIONES DATASET S.A.S.**, identificado con NIT. No **901106067,** denominada **DATASET SAS** a la fecha 27/02/2026, presenta la siguiente información:

NOMBRE PRODUCTO	NO PRODUCTO	FECHA APERTURA	ESTADO	NOMBRE SUCURSAL	NÚMERO SUCURSAL
CUENTA AHORROS	554-835098-71	2017/10/11	ACTIVA	ALTO PRADO	692

Quedamos a su disposición, por eso en caso de requerir ampliar la anterior información podrá comunicarse con su comercial o gerenciado, en el momento que lo estime conveniente.

Atentamente,

* Importante: Esta constancia sólo hace referencia a los productos mencionados anteriormente.

VIGILADO

Bancolombia