

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORIA	DESCRIPCION
1	GERENCIA	Seguimiento a la ejecución del contrato, siguiendo las mejores prácticas del PMI
1.1	Gestión del Proyecto	<p>El contratista debe presentar para aprobación del Comité un Plan de Gestión del Proyecto que debe incluir como mínimo lo siguiente:</p> <ul style="list-style-type: none"> a) <u>Documento Análisis Infraestructura Existente</u>: hardware, software, información, servicios conexos, indicadores, actores y flujo de proceso utilizado actualmente por la Entidad Territorial. b) <u>Documento Solución Propuesta</u>: determinar el hardware, software, bases de datos, desarrollos, configuraciones, parametrizaciones y demás servicios conexos necesarios para la prestación del servicio, incluido el plan de mantenimiento preventivo. c) <u>Documento Plan de Comunicaciones</u>: con el modelo de atención de PQRS, el detalle de los canales de atención (número de teléfono, correo electrónico, canales en redes sociales, etcétera), enlaces a la(s) plataformas para la gestión y monitoreo de los servicios junto a los respectivos accesos para la Entidad Territorial, así como el nombre, cédula, número de teléfono móvil y correo electrónico del Gerente de Proyecto designado. d) <u>Documento Plan de Gestión del Recurso Humano</u>: con la matriz RACI del personal que el Aliado pondrá a disposición de la Entidad Territorial, incluyendo información de contacto y soportes de hoja de vida. e) <u>Cronograma</u>: con los plazos previstos para la adquisición, instalación, configuración y puesta en funcionamiento de los servicios. f) Protocolos o manuales que serán utilizados por el operador para la configuración de sus servicios. g) Propuesta clasificación de PQRS por tipos, tema y subtemas.
1.2	Articulación e informes.	El Gerente debe adelantar y propiciar la interacción entre los diferentes actores de la solución, con los beneficiarios y con la entidad contratante. Debe articular las acciones para el desarrollo del proyecto, a través de la asistencia y liderazgo de las reuniones que se requieran para el normal desarrollo del proyecto. También debe asesorar, presentar informes y emitir los conceptos técnicos al Comité para facilitar la toma de decisiones del proyecto.
2	SOPORTE Y MESA DE AYUDA	El Aliado debe garantizar la disponibilidad de todos los recursos que sean necesarios para el diseño, implementación, puesta en funcionamiento y operación del servicio, así como también, garantizar el soporte y disponibilidad.
2.1	Mantenimientos preventivos y correctivos	El Aliado debe presentar para aprobación del Comité un " <i>Plan de Mantenimiento</i> " que permita garantizar la disponibilidad del 98% del sistema y cada uno de sus componentes.
2.2	Mesa de Ayuda	<p>Durante el plazo de ejecución del contrato y el periodo de soporte y garantía, el contratista deberá disponer de una Mesa de Ayuda con las siguientes características funcionales mínimas:</p> <ul style="list-style-type: none"> a) Brindar atención vía telefónica (fijo y móvil), chat (WhatsApp) y correo electrónico para atención en horario hábil 7*24*365. b) Generar e informar al solicitante el número de reporte por cada PQRS.

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORÍA	DESCRIPCIÓN																		
		<ul style="list-style-type: none"> c) Resolver cualquier petición, queja o reclamo que sea presentada por algún funcionario de la Entidad Territorial. d) Mantener actualizadas las guías, manuales, documentos y demás material didáctico de la solución. e) Informar mensualmente el estado de los PQRS presentados durante el periodo. <p>Los indicadores clave de rendimiento (KPI) deberán ser acordados con la supervisión en el “Documento Solución Propuesta” luego del Análisis Infraestructura Existente.</p>																		
2.3	Estrategia de uso y apropiación	El Aliado debe adelantar campañas mensuales sobre el uso y apropiación del servicio a través de llamadas, o eventos, o conferencias, o con el envío de correos electrónicos, o SMS, o WhatsApp, o con la generación de piezas de comunicación para que sean publicadas en redes sociales o por los diferentes medios de comunicación.																		
3	REPORTERÍA E INFORMES	Proveer como parte del servicio informes de analítica de datos, disponibilidad del servicio, tráfico de datos, etc.																		
3.1	Supervisión del tráfico	El servicio debe posibilitar la generación de reportes históricos sobre los hábitos de navegación de todos los usuarios de la red WiFi, como tiempos de navegación, sitios y aplicaciones más visitados (no importa si están en una categoría bloqueada o no), los sitios más buscados y reportes por categorías con información que posibilite análisis de tendencias de uso por horas, días, semanas y meses, para la correlación de datos de consumo, PQR, datos demográficos y de los usuarios.																		
3.2	Supervisión de la mesa de ayuda	<p>El servicio debe posibilitar la generación de reportes históricos sobre las incidencias y requerimientos que han sido atendidos por el personal de la mesa de ayuda, de tal manera que se puedan focalizar estrategias de atención, prevención o de sensibilización en el uso del servicio. La herramienta utilizada para la supervisión de la mesa de ayuda debe permitir la generación de tablero de control con los PQRS abiertos, incluyendo su tipología y tiempo restante para la atención siguiendo de acuerdo con lo siguientes ANS:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3" style="background-color: #FFD700;">ANS</th> </tr> <tr> <th style="width: 33%;">Prioridad</th> <th style="width: 33%;">Tiempo de respuesta estimado (horas hábiles)</th> <th style="width: 33%;">Tiempo de solución estim (horas hábiles)</th> </tr> </thead> <tbody> <tr> <td>Crítico (Interrupción Masiva del Servicio para la totalidad de los usuarios)</td> <td style="text-align: center;">2</td> <td style="text-align: center;">6</td> </tr> <tr> <td>Mayor (Interrupción Masiva del Servicio para dos o más usuarios en un mismo enlace)</td> <td style="text-align: center;">4</td> <td style="text-align: center;">8</td> </tr> <tr> <td>Menor (Interrupción del Servicio para un usuario)</td> <td style="text-align: center;">6</td> <td style="text-align: center;">24</td> </tr> <tr> <td>Cualquier otro incidente o requerimiento</td> <td style="text-align: center;">8</td> <td style="text-align: center;">72</td> </tr> </tbody> </table>	ANS			Prioridad	Tiempo de respuesta estimado (horas hábiles)	Tiempo de solución estim (horas hábiles)	Crítico (Interrupción Masiva del Servicio para la totalidad de los usuarios)	2	6	Mayor (Interrupción Masiva del Servicio para dos o más usuarios en un mismo enlace)	4	8	Menor (Interrupción del Servicio para un usuario)	6	24	Cualquier otro incidente o requerimiento	8	72
ANS																				
Prioridad	Tiempo de respuesta estimado (horas hábiles)	Tiempo de solución estim (horas hábiles)																		
Crítico (Interrupción Masiva del Servicio para la totalidad de los usuarios)	2	6																		
Mayor (Interrupción Masiva del Servicio para dos o más usuarios en un mismo enlace)	4	8																		
Menor (Interrupción del Servicio para un usuario)	6	24																		
Cualquier otro incidente o requerimiento	8	72																		
3.3	Reportes para la medición de ANS	El Aliado debe contar con las herramientas necesarias para detectar y monitorear fallas e Interrupciones en los servicios contratados. El Aliado entregará el detalle de la falla presentada y la solución realizada a la misma en los tiempos definidos en los ANS.																		

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORIA	DESCRIPCION
		<p>Para la medición de los ANS, el Aliado debe entregar reportes sobre gestión incluyendo los resultados de seguimiento hecho durante el mes de los indicadores que a continuación se listan:</p> <ul style="list-style-type: none"> - Disponibilidad. - Número máximo de interrupciones. - RTO. - MTBF. - Latencia - Ancho de banda <p>Adicionalmente, para los servicios de enlaces terrestres y satelitales el Proveedor debe monitorear las siguientes variables:</p> <ul style="list-style-type: none"> - Tráfico de entrada. - Tráfico de salida.
3.4	Paradas de reloj	El cálculo de los tiempos de los ANS no deberá tener en cuenta los plazos que son responsabilidad o sean atribuibles a terceros, a la Entidad Territorial o a los usuarios, por ejemplo: permisos de acceso, información errada, fallas de fluido eléctrico, eventos de fuerza mayor, daños o mala operación de los dispositivos.
4	PORTAL CAUTIVO ENTIDAD TERRITORIAL	Prestar el servicio de asistencia técnica y gestión completa del portal cautivo para el acceso a la red inalámbrica en las sedes educativas.
4.1	Analítica WiFi	Información centralizada, sobre la interacción de los usuarios dentro de las zonas wifi; así como, datos demográficos, tiempos de permanencia, puntos de interés, usuarios nuevos o recurrentes.
4.2	Micro Sondeos en tiempo real	Recopilación y conocimiento de datos cualitativos para perfilar de manera específica a la audiencia; como, datos demográficos, opiniones, intereses o experiencias para segmentación de la audiencia.
4.3	Microsegmentación	Generación de estrategias clave a una audiencia objetivo, que ya se conoce y ha sido segmentada; es así como la microsegmentación está orientada a hacer campañas.
5	CONECTIVIDAD SEGURA DE SD WAN ENTIDAD TERRITORIAL	<p>Prestar el servicio de conectividad SD WAN seguro a la Entidad Territorial.</p> <p>La solución debe permitir la conexión SDWAN de las dependencias con la Entidad Territorial y deben tener la posibilidad de salir al Internet Local de forma segura</p> <p>SEDES PEQUEÑAS</p> <ul style="list-style-type: none"> - Secretaría de cultura - Biblioteca - Auditorio Cultura - CEA - Casa del adulto mayor - Renacer - Clínica veterinaria - Caja social de la mujer - Agrícola (Umata) - Archivo - Inspecciones 1 y 2 <p>SEDE MEDIANA</p>

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORIA	DESCRIPCION
		<ul style="list-style-type: none"> - Cedromall <p>SEDE GRANDE</p> <ul style="list-style-type: none"> - Entidad Territorial <p>El oferente deberá estar en la capacidad de aumentar anchos de banda hasta en un 50% su capacidad según requerimiento de la entidad</p>
5.1	Canales de Internet para sedes de la Entidad Territorial denominadas pequeñas	<p>Se requiere para las sedes pequeñas servicios de conectividad en banda ancha con velocidad mínima de 100 Mbps para el canal principal</p> <p>Se requiere que las sedes cuenten con un respaldo de conectividad en banda ancha terrestre o satelital</p>
5.2	Servicios complementarios para sedes de la Entidad Territorial denominadas pequeñas	<p>La solución propuesta debe admitir un Throughput Firewall de 1 Gbps, Throughput Next-generation firewall de 300 Mbps</p> <p>La solución propuesta debe admitir un Throughput de Protección contra Amenazas de 200 Mbps</p> <p>La solución propuesta debe admitir un Throughput IPS de mínimo 600 Mbps</p> <p>La plataforma de hardware debe soportar mínimo 200.000 sesiones simultaneas y 15.000 nuevas sesiones por segundo</p> <p>La solución propuesta debe admitir un Mínimo 5 interfaces de red 10/100/1000 en cobre, formato RJ45 y 1 interfaz SFP</p> <p>La solución propuesta deberá contar con mínimo 1 puerto de consola y 1 puertos USB para administración</p>
5.3	Canales de Internet para sedes de la Entidad Territorial denominadas Mediana	<p>Se requiere para las sedes medianas servicios de conectividad de mínimo 400 Mbps en dedicado</p> <p>Se requiere que la sede cuente con un respaldo de conectividad en banda ancha terrestre o satelital</p>
5.4	Servicios complementarios para sede de la Entidad Territorial: Cedromall (sede denominada Mediana)	<p>La solución propuesta debe admitir un Throughput Firewall de 4 Gbps, Throughput Next-generation firewall de 1,2 Gbps</p> <p>La solución propuesta debe admitir un Throughput de Protección contra Amenazas de 800 Mbps</p> <p>La solución propuesta debe admitir un Throughput IPS de minimo 3,4 Gbps</p> <p>La plataforma de hardware debe soportar mínimo 300.000 sesiones simultaneas y 48.000 nuevas sesiones por segundo</p> <p>La solución propuesta debe admitir un mínimo 5 interfaces de red 10/100/1000 en cobre, formato RJ45</p> <p>La solución propuesta deberá contar con mínimo 1 puerto de consola y 1 puertos USB para administración</p>
5.5	Canales de Internet Entidad Territorial (Sede denominada Grande)	<p>Se requiere para las sedes grandes servicios de conectividad de mínimo 1000 Mbps en dedicado</p> <p>Se requiere que la sde cuenten con un respaldo de conectividad en banda ancha de 500 Mbps</p>
5.6	Servicios complementarios Entidad Territorial (Sede Denominada Grande)	<p>La solución propuesta debe admitir un Throughput Firewall de 10 Gbps, Throughput Next-generation firewall de 2,59 Gbps</p> <p>La solución propuesta debe admitir un Throughput de Protección contra Amenazas de 1,73 Gbps</p> <p>La solución propuesta debe admitir un Throughput IPS de minimo 5 Gbps</p>

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORIA	DESCRIPCION
		La plataforma de hardware debe soportar mínimo 1,500.000 sesiones simultaneas y 130.000 nuevas sesiones por segundo
		La solución propuesta debe admitir un mínimo 8 interfaces de red 10/100/1000 en cobre, formato RJ45, Mínimo 8 interfaces de red SFP
		La solución propuesta deberá contar con mínimo 1 puerto de consola y 1 puertos USB para administración
5.7	Funcionalidades generales SD WAN	Soporte para publicar servicios de Internet e Intranet
		Compatibilidad con la red VPN para ayudar a los usuarios a establecer rápidamente una red VPN y ofrecer configuraciones durante la implementación de ZTP.
		Soporte para configurar todas las interfaces efectivas de los dispositivos administrados.
		Soporte para mostrar el monitoreo del enlace de túnel y el enlace WAN.
		Soporte para configurar la prioridad de las interfaces WAN de los dispositivos SD-WAN.
		Soporte para configurar la prioridad del enlace de túnel en el negocio de intranet SD-WAN.
5.8	Prevención de Intrusiones	La solución debe ser compatible con la protección contra ataques CC con límite de solicitudes, límite de proxy, umbral personalizado y métodos compatibles con los rastreadores. Admite 4 métodos de autenticación: Cookie JS, Redireccionamiento, Confirmación de acceso, CAPCHA
		La solución debe ser compatible con la detección de anomalías de protocolo y la detección basada en velocidad.
		La solución debe admitir la opción de registro de paquetes
		La solución debe ser compatible con el perfil de seguridad IPS en función de la gravedad, el destino, el sistema operativo, la aplicación o el protocolo.
		La solución debe ser compatible con la exención de IP de firmas IPS específicas.
		La solución debe ser compatible con el modo de funcionamiento del IDS sniffer.
		La solución propuesta debe ser compatible con la reputación de IP y el bloqueo de IP del servidor de botnet con una base de datos global de reputación de IP
5.9	Filtrado de URL /Control de acceso web	La solución debe admitir el filtrado web dinámico con una base de datos de categorización en tiempo real basada en la nube: más de 140 millones de URL con no menos de 64 categorías (no menos de 8 de las cuales están relacionadas con la seguridad)
		La solución debe ser compatible con la inspección de filtrado web flow-based
		La solución debe admitir el filtrado web definido manualmente en función de la dirección URL, el contenido web y cabeceras MIME
		La solución debe admitir las siguientes características adicionales de filtrado web <ul style="list-style-type: none"> - Filtrar applet de Java, ActiveX y/o cookie - Bloquear publicación HTTP - Palabras clave de búsqueda de registro - Exento de escanear conexiones cifradas en ciertas categorías por motivos de privacidad

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORIA	DESCRIPCION
		La solución debe admitir la invalidación del perfil de filtrado de URL para permitir que el administrador asigne temporalmente diferentes perfiles al usuario/grupo/IP
		La solución propuesta debe admitir la personalización de categorías de URL
5.10	Antivirus	La solución debe admitir más de 3,3 millones de firmas antivirus, con actualizaciones manuales y automáticas de firmas push o pull
		La solución debe ser compatible con el antivirus basado en flujos: los protocolos incluyen HTTP, SMTP, POP3, IMAP4, FTP/SFTP, SMB
		La solución debe admitir la detección de virus para archivos comprimidos como RAR, ZIP, GZIP, BZIP2, TAR; Admite la detección de archivos comprimidos multicapa para no menos de 5 capas de descompresión y personaliza la acción para exceder comportamientos
		La solución debe admitir contenido de advertencia definido por el usuario para sitios web maliciosos y virus, alertar al usuario de que el sitio web es un sitio web malicioso o se ha detectado un virus
		La solución propuesta debe admitir la vinculación con la plataforma inteligente en la nube y actualizar la base de datos de virus en línea con regularidad.
		La solución propuesta debe soportar el control de acceso de sitios web maliciosos
5.11	Cloud Sandbox	La solución debe admitir la dirección de transferencia de archivos y el control de tamaño de archivo
		La solución debe admitir el bloqueo de resultados de detección para bloquear rápidamente las amenazas desconocidas.
		La solución debe ser compatible con el intercambio global de inteligencia de amenazas y el bloqueo de amenazas en tiempo real
		La solución debe admitir la función de deshabilitar la carga de archivos sospechosos, los archivos sospechosos no se cargarán automáticamente en el espacio aislado en la nube para su detección
		Compatibilidad para marcar el archivo de script como un archivo sospechoso y obtener el resultado del análisis del espacio aislado en la nube.
		La solución propuesta debe admitir la carga de archivos maliciosos en el espacio aislado en la nube para su análisis
		La solución propuesta debe proporcionar un informe completo de análisis del comportamiento del archivo para el archivo que se consideró malicioso.
5.12	WLAN	Se requieren para las sedes pequeñas la instalación de dos puntos de acceso para uso en interiores
		Se requieren para las sedes medianas la instalación de cuatro puntos de acceso para uso en interiores
		Se requieren para las sedes grandes la instalación de ocho puntos de acceso para uso en interiores
		Se proporcionar acceso a la red a funcionarios y visitantes en cada sede mediante una red inalámbrica.
		La solución propuesta deberá soportar como mínimo 100 usuarios por punto de acceso
		La solución propuesta deberá soportar como mínimo 16 SSID

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORÍA	DESCRIPCIÓN
		La solución propuesta deberá contar con la capacidad de ser administrado a través de una plataforma virtual en la nube proporcionada por el mismo fabricante.
		Los puntos de acceso deberán contar con antenas integradas
		Los puntos de acceso deberán tener la capacidad de disminuir la interferencia mediante el uso de antenas direcciones
		Los puntos de acceso deberán encontrar de forma dinámica los canales de Wi-Fi menos congestionados que estén disponibles
		Los puntos de acceso deben cumplir mínimo con los estándares IEEE 802.11a/b/g/n/ac
		Los Equipos deben ser alimentados por PoE acorde IEEE 802.3af
		Debe contar con certificación Wi-Fi Alliance
5.13	Office	400 cuentas de Office 365 E1
5.14	Troncales IP	35 troncales para centro administrativo 5 Troncales para CAMVIC
6	ANALÍTICA Y FILTRADO DE CONTENIDO WEB PARA INSTITUCIONES EDUCATIVAS	Proveer un servicio de filtrado de contenido web avanzado, diseñado para gestionar y controlar el acceso a la información en la web.
6.1	Categorías y dominios a restringir	El servicio de filtrado debe soportar por lo menos 70 categorías entre las cuales se encuentran: pornografía, aborto, juegos y apuestas, armas, drogas, crimen, delitos, chat, hacking, astrología, violencia, entre muchas más
6.2	Bloqueo de dominios específicos	Permitir o denegar el acceso a dominios específicos, por ejemplo en situaciones donde la confianza en ciertos sitios web no está garantizada, se puede tomar la medida de denegar el acceso,
6.3	Análisis del Tráfico	Tanto para el filtrado de contenido, como para el proceso de extracción de datos sobre uso del servicio, el Aliado debe utilizar herramientas y dispositivos lo suficientemente robustos que no afecten el rendimiento ni la disponibilidad del servicio.
6.4	Resultado de la Analítica de Datos	Producto de la analítica de los datos de consumo, la Entidad Territorial podrá solicitar a Aliado la incorporación de categorías, dominios, aplicaciones o páginas web específicas dentro del filtrado de contenido en cualquier momento durante la ejecución del contrato.
7	CONECTIVIDAD PARA INSTITUCIONES EDUCATIVAS	<p>Prestar el servicio de Internet dedicado, redundancia, soporte y administración para asegurar una conexión a todos los usuarios en las sedes educativas.</p> <p>SEDES PEQUEÑAS:</p> <ul style="list-style-type: none"> - Jardín infantil sol Solecito - Escuela Ruperto - parcelas - Escuela Rozo - Escuela Abra - Escuela La Moya - Escuela Pueblo viejo - Escuela Ubamux - Casa Nadi <p>SEDES GRANDES:</p> <ul style="list-style-type: none"> - IED EPP

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORÍA	DESCRIPCION
		<ul style="list-style-type: none"> - Camilo Torres - IED Parcelas
7.1	Canales internet dedicado en sedes educativas	<p>Proveer servicios de Internet dedicado (reúso 1:1) para las sedes denominadas como Grandes y proveer el servicio de Internet Banda Ancha para cada una de las sedes educativas denominadas como pequeñas, a través de conexiones de fibra óptica de acuerdo con la cantidad de dispositivo o usuarios <u>administrativos</u> concurrentes, así:</p> <ul style="list-style-type: none"> • Sede pequeña: De 1 a 50 dispositivos concurrentes: 100 Mbps Banda Ancha • Sede grande: De 51 o más dispositivos concurrentes: 100 Mbps Dedicados (Camilo Torres, IE Parcelas; IE Distrital EPP) <p>En todo caso el Aliado deberá monitorear permanentemente los enlaces para validar la saturación del canal, de tal manera que sea posible sustentar la ampliación o reducción de los canales para ceñirse a las necesidades de la Entidad Territorial.</p> <p>El oferente deberá estar en la capacidad de aumentar anchos de banda hasta en un 50% su capacidad según requerimiento de la entidad.</p>
7.2	Canal de internet de respaldo para Instituciones educativas	<p>Proveer el servicio de Internet de respaldo de mínimo 100 Mbps vía satelital o fibra óptica, con un operador diferente, a las 3 sedes educativas con más de 50 usuarios/dispositivos concurrentes. (Camilo Torres, IE Parcelas; IEDistrital EPP)</p>
7.3	Administrador de Ancho de Banda	<p>Administrar y soporte del ancho de banda para cada una de las sedes educativas, aplicando políticas de QoS</p>
7.4	Hardware y software	<p>El Aliado debe garantizar toda la conectividad física y lógica requerida para la puesta en funcionamiento de los servicios y conectividad contratada.</p> <p>Los bienes, productos y equipos se entregan en calidad de servicio, razón por la cual la Entidad Territorial adquiere en comodato la custodia temporal y es responsable de la devolución de equipos en buen estado.</p> <p>La conectividad física hace referencia a todos los elementos de hardware necesarios para proveer el servicio. La conectividad lógica hace referencia a todos los elementos de software necesarios y su respectiva configuración para proveer el servicio.</p>
7.5	VPN	<p>La Entidad Territorial en cualquier momento durante la ejecución del contrato podrá requerir las VPN's IPsec (Client-to-Site o Site-to-Site) y SSL (Client-to-Site) que requiera, destinando el ancho de banda que técnicamente se recomienda para tales fines sin afectar la calidad de servicio de los usuarios.</p>
7.6	IP	<p>El Aliado deberá proporcionar las direcciones IPv4 y/o IPv6 compatibles, necesarias que garanticen publicar y prestar los servicios de la Entidad Territorial dentro del alcance del presente contrato. El Aliado debe garantizar que todos los componentes de los servicios de conectividad soporten y sean compatibles tanto en IPv4 e IPv6.</p>
7.7	Daños o mal funcionamiento de los equipos	<p>El Aliado debe reemplazar los equipos que hacen parte del servicio cuando se presentan daños o mal funcionamiento de tal forma que pueda cumplir con los ANS establecidos. En los casos en que el daño sea atribuible a la Entidad Territorial por manipulación indebida o cambios no acordados con el Aliado de las condiciones en que fueron instalados los equipos, la Entidad Territorial asumirá los costos de la reparación de los equipos.</p>

ANEXO-1 CONDICIONES TÉCNICAS

ITEM	CATEGORÍA	DESCRIPCIÓN
7.8	Adecuaciones	El Aliado deberá adelantar las adecuaciones físicas menores: constructivas, eléctricas y ambientales que posibilite la instalación y operación adecuada de sus dispositivos.
7.9	Inicio de operación y pruebas	El Aliado debe coordinar con la supervisión la fecha y lugar exacta para la instalación de los servicios que sólo podrán ser facturados luego de la aceptación de las pruebas por parte del supervisor, las cuales deben incluir como mínimo: <ul style="list-style-type: none"> - Ping a sitio remoto. - Navegación a sitio web externo. - Prueba de navegación a un sitio restringido. - Verificación de la velocidad de subida y de bajada. Dichas pruebas deberán generar un acta con la evidencia de la ejecución (fotos, grabaciones o capturas de pantalla).
8	CONECTIVIDAD ADMINISTRADA	Prestar el servicio de soporte y administración de la solución de WLAN para las sedes educativas
8.1	Servicio de gestión y administración de conectividad LAN/WLAN en sede	Prestar el servicio administración y soporte de red WLAN, siendo necesario que el CONTRATISTA garantice la disponibilidad del servicio a las distintas sedes
8.2	Puntos de acceso para sedes	Prestar el servicio de puntos de acceso inalámbrico 802.11ac, así: <ul style="list-style-type: none"> • Sedes pequeñas: 1 punto para interiores y 1 para exteriores • Sedes grandes: 2 puntos para interiores y 1 punto para exteriores Cada punto debe tener capacidad mínima de hasta 100 usuarios.
8.4	Gestión centralizada	Ofrecer servicios de gestión centralizada para todos los puntos de acceso desde una única controladora en la nube del mismo fabricante de los AP.
8.5	Infraestructura	Deberá incluir en su servicio, materiales y consumibles para la instalación y puesta en marcha de la red WLAN.
9	PORTAL CAUTIVO PARA INSTITUCIONES EDUCATIVAS	Prestar el servicio de asistencia técnica y gestión completa del portal cautivo para el acceso a la red inalámbrica en las sedes educativas.
9.1	Analítica WiFi	Información centralizada, sobre la interacción de los usuarios dentro de las zonas wifi; así como, datos demográficos, tiempos de permanencia, puntos de interés, usuarios nuevos o recurrentes.
9.2	Micro Sondeos en tiempo real	Recopilación y conocimiento de datos cualitativos para perfilar de manera específica a la audiencia; como, datos demográficos, opiniones, intereses o experiencias para segmentación de la audiencia.
9.3	Microsegmentación	Generación de estrategias clave a una audiencia objetivo, que ya se conoce y ha sido segmentada; es así como la microsegmentación está orientada a hacer campañas.

ACTIVIDAD	RESPONSABLE	FIRMA
Elaboró	Carlos Burbano Barrera/Director Jurídico	
Revisó	Alejandro Garzón / Gerente técnico y operativo	
Aprobó	Andrés Escobar T./ Director Técnico y Operativo	