OBJETO: SUMINISTRO E IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS ORIENTADAS AL FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA, CONECTIVIDAD Y SEGURIDAD DIGITAL EN EL MARCO DEL PROYECTO "FORTALECIMIENTO A LA GESTIÓN, PROCESOS Y PROGRAMAS TRANSVERSALES DE LA DIRECCIÓN DE TRÁNSITO DEL MUNICIPIO DE BUCARAMANGA".

El contratista deberá cumplir con el objeto del contrato y entregar a la entidad los elementos de la siguiente ficha de especificaciones técnicas dentro del plazo establecido, elementos que deben cumplir con las especificaciones:

DESCRIPCION DEL SERVICIO	Cant
COMPONENTE 1: Software Gobierno Digital	
1.1 Suministro, configuración y puesta en funcionamiento de un software gestor de proyectos para la gestión de contenido de la entidad para cumplimiento de la política de gobierno digital como servicio en la nube	1
COMPONENTE 2: Transición Ipv4 a Ipv6 y análisis de vulnerabilidades	
2.1 3 Desarrollo de las 3 fases necesarias para la transición del protocolo IPv4 a IPv6 en cumplimiento de la normativa vigente	1
2.2 Realización del análisis de vulnerabilidades sobre la infraestructura tecnológica institucional	1
COMPONENTE 3: Fortalecimiento de infraestructura de red	
Red de datos cableada	1
Red de datos inalámbrica	1

COMPONENTE 1: SOFTWARE GOBIERNO DIGITAL

La plataforma constituye un ecosistema digital diseñado para el control, organización y aseguramiento de la documentación técnica y administrativa de alta criticidad. El sistema está optimizado para actuar como el repositorio central en proyectos de modernización de infraestructura, permitiendo la trazabilidad completa de manuales, protocolos de red y esquemas de direccionamiento durante la coexistencia y transición de protocolos.

Debe ser un software totalmente gráfico e intuitivo, de fácil manejo y parametrización.

Debe tener Funcionamiento 100% WEB y en la nube (SaaS).

Debe ser compatible con todos los motores de bases de datos (ORACLE, SQL SERVER, POSTGRESS, MYSQL,etc.).

La solución debe garantizar estabilidad y confiabilidad.

El funcionamiento en Ambiente Web, no debe requerir instalación de plugins, applets, o similares para que el software funcione y debe poder funcionar en cualquier navegador (mozilla, crome, safari, opera, etc).

Debe poder usarse en cualquier dispositivo con cualquier sistema operativo, siempre y cuando se cuente con un navegador y conexión a internet sin requerir instalación de ninguna aplicativo.

El software debe realizar la validación del ingreso del usuario por medio de nombre de usuario y contraseña.

Debe permitir crear los tiempos de validez del usuario teniendo en cuenta el tiempo del contrato de los mismos.

Debe permitir la creación de horarios de trabajo para los usuarios.

El control al ingreso de los módulos y de cada uno de los menús debe ser paramatrizable para cada usuario del sistema.

Debe generar reportes y logs de auditoria indicando el usuario que realizó una actividad dentro del sistema, así como la fecha y hora.

Las claves de los usuarios deben mantenerse encriptadas y no se guardaran en la base de datos ni archivos externos.

La recuperación de las claves s debe hacer a través del correo institucional de cada usuario lo que garantiza que solo el podrá recuperarla.

El sistema debe generar alerta de cambio de clave como se parametrice en el sistema para que los funcionarios estén cambiando periódicamente las claves de la base de datos

El sistema debe crear perfiles y roles en la base de datos de tal forma que el administrador no requerir entrar a la base de datos para Realiza tareas de tipo administrativo.

Debe tener manejo de Permisos especiales a ciertas Funcionalidades

Debe tener la capacidad de generar una taxonomía de información multinivel. Cada nodo (carpeta) admite la parametrización de un código de identificación técnico, facilitando la alineación con los estándares de gestión documental institucional.

Debe permitir la carga de identificadores gráficos (logos o iconos) por contenedor, lo que agiliza la ubicación visual de áreas críticas.

Debe tener un sistema de carga de archivos con validación de extensión y tamaño. Permite la actualización de documentos existentes manteniendo la coherencia de la base de datos.

Debe tener la integración de herramientas de descarga directa y previsualización de registros para una respuesta rápida en procesos de soporte técnico.

El administrador del sistema debe tener la capacidad de asignar privilegios específicos (Lectura/Escritura/Gestión) a nivel de carpeta. Esto garantiza que la información sensible de la transición de red solo sea accesible por el personal de ingeniería autorizado.

Implementación de ventanas emergentes (pop-ups) de confirmación para acciones críticas (eliminación o anulación), evitando la pérdida accidental de datos.

El sistema debe estar diseñado para soportar la carga documental que conlleva un cambio de paradigma de red, permitiendo:

- Almacenamiento organizado de inventarios de dispositivos compatibles con Dual-Stack.
- Centralización de las nuevas políticas de seguridad y tablas de enrutamiento IPv6.
- Repositorio de manuales de administrador y guías de configuración de equipos de borde, asegurando que el conocimiento técnico sea transferible y esté siempre disponible.

Se debe incluir el servidor en la nube con las siguientes características mínimas durante la duración del contrato y un año más.

Procesador de 8 nucleos
Memoria de 16 gb de Ram
Disco SSD de 512 GB

Debe incluir capacitación, instalación y puesta en marcha

Debe incluirse soporte y mantenimiento por doce (12) meses adicionales posterior a la finalización del contrato.

COMPONENTE 2: Transición Ipv4 a Ipv6 y análisis de vulnerabilidades

En el desarrollo del objeto contractual, el contratista deberá cumplir con cada una de las fases, requerimientos, lineamientos y plantillas establecidas por el MINTIC, en las Guía de transición de IPv4 a IPv6 para Colombia y la Guía para el aseguramiento del Protocolo IPv6, así como la realización de un análisis de vulnerabilidades a la infraestructura a través de un escaneo controlado que arroje el diagnostico de riesgos en los que se encuentra la entidad.

FASES DE TRANSICIÓN IPv4 a IPv6

El proceso deberá desarrollarse en cumplimiento de la Resolución 2710 de 2017, modificada por la Resolución 1126 de 2021, y en concordancia con el Decreto 1078 de 2015.

A. Fase I. Planeación de IPv6.

Debe realizarse un diagnóstico de la infraestructura tecnológica de la DTB, teniendo en cuenta que se analiza el inventario de activos informáticos, se identifican parámetros críticos señalados en el modelo de referencia para la adopción de IPv6.

Las siguientes son las actividades a tener en cuenta en esta fase:

a. Elaborar y validar el inventario de activos de información de servicios tecnológicos de la DTB y su interrelación entre ellos, de acuerdo al inventario de hardware y software, identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6.
b. Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de la DTB con base en lo establecido en el inventario de activos de información.
c. Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en la DTB; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI de la DTB de tal manera que la información recogida de esta tarea sea insumo para el inicio de la fase II de IPv6.
d. Identificar la infraestructura física en su totalidad, actualmente en la DTB en funcionamiento, topología actual de la red física y lógica, su esquema de direccionamiento IPV4 implementado, dispositivos activos de red (switch core, switches de borde, Access Point (Wi-Fi)), dispositivos de seguridad (firewalls, entre otros), Servidores (sistema operativo del servidor), servicios de red (DNS, DHCP, HTTP, entre otros), especialmente la arquitectura inherente a cada servicio, aplicaciones en red, servidores en cloud de Google, estaciones de usuarios (sistemas operativos), elementos del Proveedor de Servicios de Internet (ISP), y su funcionamiento dentro de la organización y con base en esto, proponer el nuevo diseño de red sobre IPv6, dando cumplimiento con la normatividad vigente.
e. Generar el plan detallado del proceso de transición de esta fase hacia IPv6 con base en el plan de diagnóstico y el diseño de la red de comunicaciones.
f. Planear el proceso de transición de los servicios tecnológicos con que cuenta la entidad. Especificar que cumple y que no cumple.
g. Validar el estado actual de los sistemas de comunicaciones, los sistemas de almacenamiento y evaluar la interacción entre ellos para cuando se adopte el protocolo IPv6.
h. Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no pueden soportar IPv6. Para cada activo el contratista debe constatar con los fabricantes y con los terceros si es necesario, el cumplimiento de IPv6, a través de la certificación y/o datasheet que avale el soporte del nuevo protocolo en éstos.
i. Identificar la configuración y todos los esquemas de seguridad de la red de comunicaciones y sistemas de información, en coexistencia con los dos protocolos.
j. Revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente esté plenamente controlado a través de

zonas desmilitarizadas desde el firewall respectivo de la DTB, de acuerdo a los RFC correspondientes a políticas de enrutamiento y seguridad de IPv6.

k. Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, equipos de cómputo, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 para la DTB.

l. Preparar una zona controlada para realizar pruebas de funcionalidad del nuevo protocolo de comunicaciones IPv6.

m. Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el plan de transición.

n. Preparar a los funcionarios del Área de Sistemas, de conformidad con los planes de capacitación establecidos para el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto en la implementación del nuevo protocolo, de conformidad con el modelo de referencia de adopción de IPv6 definido en la Guía Transición.

o. Entrar en sincronización y operación con los ISP (Proveedores de Servicios de Internet) con el fin de definir las estrategias de enrutamiento de IPv6 nativo.

p. Diseñar el Plan de direccionamiento de IPv6 del prefijo solicitado previamente ante (LACNIC o Proveedor del Servicio de Internet) y elaborar en detalle el proceso de segmentación entre los distintos dispositivos y servicios de la red, teniendo en cuenta los esquemas de enrutamiento ya sea por ejemplo en /64, /56, /48, /44, según sea el caso y las necesidades de la DTB.

q. Cubrir requerimientos de capacidad IPv6 para futuros usuarios, asegurando que se tiene capacidad para la implementación, teniendo en cuenta la sede principal y sus dos plantas.

r. Establecimiento de los posibles cambios recomendados en la topología de red para evitar potenciales problemas con la transición a IPv6:

s. Estado del diagrama físico y lógico de red, analizando los posibles cambios recomendados en la topología de red para evitar posibles problemas con la transición a IPv6.

t. Análisis del direccionamiento de red actual, enumerando el total de VLANs, direccionamiento y direccionamiento público utilizado.

u. Estado de los equipos de red LAN, sus interconexiones entre centrales de cableado, y cascadas entre los switches de borde, verificación del versionamiento, modelo de equipos y documentación referente al soporte de Dual Stack para la transición y convivencia de las plataformas IPv4 e IPv6.

v. Documentación de las versiones de software a adquirir para garantizar soporte de IPV6 en aplicaciones, servicios y sistemas operativos.

w. Identificación de aplicaciones y servicios que funcionarán en IPv6.

x. Elección del mecanismo de transición.

y. Establecer un Plan de Contingencias para IPv6 que contemple los servicios críticos de la red y las aplicaciones, para que en caso de fallas al momento de implementar IPv6, se tenga el respaldo correspondiente y así mitigar posibles caídas del servicio. Generar matriz de riesgos.

Entregables de esta Fase:

Plan de trabajo para la adopción de IPv6 en toda la organización.

Plan de diagnóstico que debe contener los siguientes componentes:

Inventario de TI (Hardware y software) de la DTB.

Informe de cumplimiento de IPv6 por cada elemento de hardware y software (Red de comunicaciones, sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros).

Recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6.

Informe con el plan de direccionamiento en IPv6.

Plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6.

Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones (Que tan preparada se encuentra la entidad en tema de adopción de IPv6).

Documento que define los lineamientos de implementación de IPv6 en concordancia con la política de seguridad de información y los controles de seguridad informática de la DTB.

B. Fase II. Implementación del protocolo IPv6:

Para la implementación del protocolo IPv6, el contratista deberá realizar las siguientes actividades:

a. Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la primera Fase del proceso de transición de IPv4 a IPv6, teniendo en cuenta el inventario de los activos de información de cada una de las infraestructuras de TI de la DTB y teniendo en cuenta el diseño de la red bajo IPv6 previamente definido en la Fase I.
b. Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs creadas, con un número especial de usuarios que aprovechen la homogeneidad de la red, con servicios de filtrado, críticos a fin de evitar traumatismos en el normal funcionamiento de la red.
c. Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en Doble Pila; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.
d. Aplicar el modelo de transición de IPv6 definido, permitiendo la coexistencia de los aplicaciones, infraestructuras y servicios bajo los protocolos tanto de IPv4 como de IPv6, en modalidad de transición en doble pila.
e. Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 bajo doble pila; esta deberá permitir que tanto los servicios de IPv4 como los servicios de IPv6 funciones de manera independiente pero coexistente dentro de la DTB.
f. Validar la funcionalidad en IPv6 en los diferentes servicios y aplicaciones de la DTB sobre IPv6.
g. Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea la DTB, como lo son servidores AAA, firewalls, NAC, y equipos perimetrales de conformidad, zonas desmilitarizadas, con los RFC de seguridad en IPv6; al respecto, se recomienda revisar los RFC de seguridad en IPv6 asociados.
h. Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral, desde el interior de las redes LAN, hacia el exterior de las redes WAN a fin de garantizar que la DTB pueda generar tráfico de IPv6 nativo ante la comunidad de Internet.

Entregables de esta Fase:

Preparación y presentación del Informe del plan detallado de implementación del nuevo protocolo.
Documento con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta fase, incluyendo las configuraciones a realizar sobre el canal (canales) de comunicaciones con acceso a internet.
Informe de configuración de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

C. Fase III. Pruebas de funcionalidad de IPv6:

Deberá el contratista en esta fase final, ejecutar las pruebas de funcionalidad; para lo cual deberá desarrollar las siguientes actividades:

a. Realizar las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la DTB en un

ambiente que permita empezar a generar tráfico de IPv6 de la entidad hacia Internet y viceversa.

b. Realizar las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones y presentar el Informe de las pruebas realizadas.

c. Al momento de las pruebas de funcionalidad se debe realizar el afinamiento de las configuraciones de hardware, software y servicios de las entidad, con base en la información resultante de la fase II.

d. Elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

Entregables de esta Fase:

Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación.

Acta de cumplimiento a satisfacción de la DTB con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación.

Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

Análisis de Vulnerabilidades

El contratista deberá realizar un (1) análisis integral de vulnerabilidades que incluya como mínimo:

- Infraestructura de red (firewalls, switches, routers y dispositivos perimetrales).
- Servidores físicos y/o virtuales.
- Sistemas operativos tipo servidor.
- Servicios y puertos expuestos a internet.
- Infraestructura en la nube (si aplica).
- Activos críticos definidos por el Supervisor.

El servicio corresponderá exclusivamente a escaneo, identificación y análisis de vulnerabilidades. El análisis no incluye pruebas de penetración, explotación activa, ingeniería social ni ataques de denegación de servicio. El contratista no realizará actividades que comprometan la disponibilidad, integridad o confidencialidad de la infraestructura institucional.

Especificaciones mínimas:

El contratista deberá:

- Utilizar herramientas especializadas y debidamente licenciadas.
- Aplicar metodología alineada con estándares como ISO/IEC 27001, NIST, OWASP y CVSS.
- Clasificar las vulnerabilidades en niveles de criticidad (Crítica, Alta, Media y Baja).
- Formular recomendaciones técnicas claras de mitigación.
- Ejecutar el análisis sin afectar la operación institucional.
- Suscribir acuerdo de confidencialidad.
- Garantizar la reserva de la información obtenida.

Productos y Entregables:

El contratista deberá entregar:

1. Plan de trabajo aprobado por el Supervisor.
2. Inventario de activos evaluados.
3. Informe técnico detallado que incluya:
    - Resumen ejecutivo.

- Metodología aplicada.
- Herramienta utilizada.
- Resultados consolidados.
- Clasificación de vulnerabilidades.
- Evidencias técnicas.
- Recomendaciones de mitigación.

4. Presentación ejecutiva de resultados.

COMPONENTE 3: Fortalecimiento de infraestructura de red

Red de datos cableada

El contratista deberá realizar el fortalecimiento, complementación y modernización del sistema de cableado estructurado existente de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, en el marco de la segunda fase de intervención, teniendo en cuenta que previamente se ejecutó una Fase I mediante la cual se adelantó una adecuación parcial de la infraestructura.

En consecuencia, las actividades objeto del presente proceso deberán articularse técnica y funcionalmente con la infraestructura instalada en la fase anterior, garantizando interoperabilidad, homogeneidad tecnológica, continuidad operativa y estandarización del sistema.

La solución deberá asegurar condiciones de flexibilidad, escalabilidad y protección frente a la obsolescencia tecnológica, así como una operación centralizada con bajos requerimientos de mantenimiento, garantizando alta funcionalidad y operabilidad de la red institucional.

El diseño y las adecuaciones que se implementen deberán ejecutarse bajo estándar mínimo Categoría 6A UTP o superior y/o fibra óptica, conforme a las normas técnicas vigentes, buenas prácticas de cableado estructurado y especificaciones del fabricante, asegurando compatibilidad con la infraestructura previamente instalada..

Diseño y criterios técnicos

El proponente deberá estructurar su propuesta conforme a la tecnología ofrecida y a los requerimientos establecidos en el presente anexo, los cuales constituyen la funcionalidad mínima exigida por la Entidad.

El sistema deberá:

- Soportar aplicaciones bajo estándar IEEE 802.3 10/100/1000/10000 Mbps Ethernet.
- Cumplir con las normas ANSI/TIA/EIA 568 vigentes.
- Garantizar compatibilidad total entre componentes..
- Contar con certificación de laboratorio independiente ETL.
- Permitir escalabilidad futura sin afectar la infraestructura instalada.

El sistema de cableado estructurado deberá ser monomarca en sus componentes pasivos, con el fin de garantizar interoperabilidad certificada, soporte integral del fabricante y emisión de garantía extendida del sistema.

Componentes mínimos del sistema

El sistema de cableado estructurado estará compuesto, como mínimo, por los siguientes elementos:

- Cable UTP Categoría 6A o superior.
- Patch cords certificados de fábrica (área de trabajo y patch panel), categoría 6A o superior.
- Jacks de telecomunicaciones (monomarca categoría 6A o superior).
- Faceplates monomarca.
- Patch panels o herrajes categoría 6A o superior.
- Cables de fibra óptica (cuando aplique).

- Organizadores horizontales y verticales.
- Racks o gabinetes de telecomunicaciones.
- Bandejas para rack.
- PDU (Power Distribution Unit)
- Ductos y canalizaciones en EMT.
- Bandejas en malla para conducción de cableado.
- Cualquier otro accesorio requerido para la correcta puesta en funcionamiento.

Instalación y certificación

El contratista deberá:

- Entregar, instalar, identificar (marquillar) y certificar todos los puntos de red.
- Garantizar que cada punto esté conectado al respectivo cuarto de telecomunicaciones.
- Realizar marcación en patch panel, face plate, patch cord y wall cord.
- Certificar los puntos conforme a estándar de cableado estructurado.
- Garantizar que los patch cords sean certificados de fábrica y de igual calidad al cableado horizontal.
- Asegurar que los conectores cuenten con mecanismo integral de bloqueo conforme a norma ANSI/TIA/EIA 568.

Los puntos que superen la distancia máxima permitida por el fabricante deberán contemplar solución en fibra óptica o implementación de rack intermedio de repotenciación, incluyendo todos los accesorios y equipos necesarios.

Canalizaciones y adecuaciones

La ductería deberá ejecutarse en tubería EMT y bandeja tipo malla metálica, dimensionadas conforme al número total de puntos del contrato.

En caso de requerirse accesorios adicionales para la correcta instalación (bandejas, cables de poder especiales u otros), estos deberán estar incluidos en la propuesta. De no estar contemplados, serán asumidos por el contratista sin costo adicional para la Entidad.

Racks y gabinetes

Los gabinetes deberán:

- Tamaño de 11 RU.
- Permitir anclaje en piso o pared.
- Contar con puerta frontal en vidrio templado de seguridad de 4 mm o malla metálica.
- Incorporar barraje aislado para conexión a tierra.
- Incluir llave de seguridad.
- Garantizar espacio suficiente para maniobrabilidad y correcto funcionamiento de equipos activos y pasivos.

Todos los elementos activos y pasivos deberán quedar alojados al interior del rack de telecomunicaciones.

Planos y documentación

El contratista deberá presentar:

- Planos topológicos horizontal y vertical.
- Ubicación de centros de cableado.
- Diagramas de red.
- Rutas de canalización.
- Ubicación de racks y gabinetes.
- Certificación de puntos instalados.

- Memoria técnica de la solución implementada.

PUESTA EN FUNCIONAMIENTO DE ADECUACIONES

Descripción RED DE DATOS HORIZONTAL	Requerimiento Mínimo Solicitado: Adecuación de puntos de red de datos (Cableado Horizontal).
Cantidad	80 puntos de red de datos
Cableado estructurado	Cable UTP o FTP de 4 pares conformado por cobre sólido desde No. 23 AWG, debidamente aislados, trenzados en pares y cubiertos en chaqueta retardante al fuego y debe proporcionar características de rendimiento iguales o mayores que la categoría 6A en todos los parámetros solicitados por la norma 568 A.
	El cable deberá estar debidamente identificado al inicio y finalización de su recorrido con marquilla enrollable que no maltrate el cable dicha marcación debe identificar si es de datos y el número a que pertenece.
	Todo el cable suministrado deberá ser del mismo color.
	El sistema de cableado estructurado debe estar aprobado para proporcionar un ancho de banda de al menos 100 MHz en cada par, Ethernet 1000BASE-T.
	El sistema debe estar soportado en las áreas de distribución dispuesta en la entidad, de manera tal que los nuevos equipos a instalar se integren al sistema da cableado
	Debe cumplir o superar las especificaciones de las normas ISO/IEC11801, TIA/EIA 568.D, ETL No.103194824CRT-001, IEC 60332-1C, IEC 60332-3A, IEC 60754 e IEC 61034., IEEE 802.3an (10G-BaseT) y 802.3af/at (Especificaciones completas de alimentación PoE).
	El cableado debe este certificado con 100% Cobre
	La canalización debe ser en malla y tubería EMT, deberá contar con la protección y aterrizaje a tierra para el cableado estructurado en todo el recorrido interior cumpliendo con las normas vigentes.
	Las bandejas portacables tipo malla, en hilo de acero deben ser fabricadas con un diámetro de hilo mínimo: 4,0 mm para las bandejas porta cables hasta anchos de 100 mm 4,5 mm para las bandejas porta cables de anchos 150 mm y 200 mm. 6,0 mm para las bandejas porta cables de anchos 300 mm hasta anchos de 600 mm. Todas las bandejas portacables serán fabricadas con un borde de seguridad longitudinal soldado en T excepto el 30x50 mm. La malla o cuadricula de la bandeja portacables es de 50 mm x 100 mm. Todas las formas serán implementadas directamente sobre el sitio, siguiendo las indicaciones del fabricante no se necesitan figuras prefabricadas.
	Los diferentes tramos de bandejas portacables serán

	ensamblados entre ellos por un sistema de unión rápida o un sistema de enlaces. Por encima de anchos de 300 mm una unión suplementaria será situada al fondo de la bandeja. Las uniones tendrán el mismo tratamiento de superficie que la bandeja portacables.
	Las bandejas portacables serán instaladas con un vano máximo de 2,5 m y no deberán pasar las cargas máximas indicadas por el fabricante
	En los cruces de cables se debe mantener una adecuada organización (peinado) de los tramos de cables Con amarres en Velcro para mantener la organización e identificación de los cables que ingresan o salen de la canalización.
Patchcords	Tipo de Cable Cat 6A S/FTP
	Esquema de Cableado T658B
	Chaqueta LSZH
	Tipo de Conector 8P8C RJ45 Blindado
	El Oferente debe suministrar dos Patchcords UTP en la misma categoría del cableado horizontal utilizado para cada punto de red
	Tipo de Conector RJ45
Certificación	Se debe entregar por parte del Oferente la certificación de los puntos de red instalados
Marquillado	Todos los puntos deben estar correctamente marquillados, Se debe identificar y gestionar el sistema de cableado estructurado de acuerdo con la norma TIA/EIA 606A o su equivalente en el momento de la adecuación.
Accesorios	Los gabinetes deben ser cerrados tipo servidor, para servicio pesado con capacidad de alojar equipos de 42 RU y 24 RU, dependiendo del dimensionamiento de equipos a instalar. Los gabinetes o rack deben cumplir con la norma EIA-310 y ANSI/TIA RS-310-D. Los gabinetes o racks deberán tener las dimensiones estándar y adecuadas para alojar Switch y Router estándar de 19 pulgadas. Los organizadores de cable horizontal 2U monomarca Los patch panels o herrajes deben ser de 48 puertos RJ45 categoría 6A, para efectos de organización por cada patch panel o herraje de 48 puertos se debe manejar un organizador de 2U. Jack conector Cat 6A para cada punto de red.
Area	Los puntos de red de datos se instalarán en los diferentes pisos de la entidad según el estudio realizado por la oficina de

	sistemas.

ADECUACIONES Y CONFIGURACIÓN DE LA SOLUCIÓN

Características	Descripción
Cableado Horizontal	Adecuaciones de cable UTP Categoría 6A 100% cobre para 70 puntos de red distribuidos en todos los pisos.
Paneles de Conexión	Patch panels de 48 puertos RJ45, categoría 6A, con organizadores de cables de 2U para cada panel instalado.
Canalización	Uso de bandejas tipo malla y tuberías EMT con protección y aterrizaje eléctrico para todo el cableado.
Racks o Gabinetes	Gabinetes (11 RU), con sistemas de ventilación, cerradura, y multitomas internas.
Certificación	Pruebas de rendimiento y certificación de todos los puntos según las normas TIA/EIA-568 e ISO/IEC 11801.
Identificación y Marcación	Etiquetado de puntos de red, Patch cords, faceplates, y conexiones en los racks y paneles.
Accesorios	Incluye faceplates, organizadores, bandejas, ductería y cualquier otro elemento necesario para las adecuaciones.
Normativas	Cumplimiento de RETIE, RoHS, y estándares internacionales de calidad y seguridad.
Documentación	Entrega de planos topológicos horizontales y verticales, y diagramas de canalización y ubicación de puntos.

Red de datos inalambrica

La solución deberá cubrir las áreas internas del edificio principal, conforme al diseño de cobertura aprobado por el Supervisor del contrato, garantizando niveles adecuados de señal, capacidad de usuarios concurrentes y estabilidad del servicio.

La solución deberá ser plenamente interoperable con la infraestructura de red existente y no podrá requerir reemplazo obligatorio de equipos activos previamente instalados, salvo recomendación técnica debidamente sustentada.

Especificaciones técnicas mínimas de los puntos de acceso (AP)

Los equipos ofertados deberán cumplir como mínimo con las siguientes características:

- Tecnología WiFi 7 (IEEE 802.11be) como estándar mínimo exigido.
- AP de doble banda o superior (2.4 GHz y 5 GHz y/o 6 GHz según aplique a WiFi 7).
- Soporte de tecnologías avanzadas como MU-MIMO y OFDMA.
- Capacidad técnica certificada por fabricante para mínimo 300 usuarios concurrentes
- Soporte mínimo de ocho (8) SSID simultáneos.
- Compatibilidad con alimentación PoE bajo estándar 802.3af / 802.3at o superior.
- Diseño para ambientes interiores.

Los puntos de acceso deberán cumplir como mínimo con el estándar IEEE 802.11be (WiFi 7) certificado por la Wi-Fi Alliance o equivalente, soportando operación en bandas 2.4 GHz, 5 GHz y 6 GHz cuando aplique en Colombia

No se aceptarán tecnologías inferiores al estándar IEEE 802.11be (WiFi 7), por cuanto la Entidad requiere una solución con proyección tecnológica mínima a cinco (5) años, garantizando mayor capacidad de usuarios concurrentes, menor latencia y compatibilidad futura con dispositivos emergentes.

Gestión y control

La solución deberá incluir:

- Controladora en la nube o sistema de administración centralizada.
- Licenciamiento incluido durante la vigencia contractual.
- Gestión centralizada de configuración y monitoreo.
- Integración con VLAN existentes.
- Implementación de portal cautivo para red de visitantes.
- Autenticación mediante servidor RADIUS y/o integración con Directorio Activo (Active Directory).
- Segmentación de red entre usuarios administrativos y visitantes.

Seguridad

La solución deberá garantizar como mínimo:

- Encriptación WPA3-Enterprise.
- Políticas de autenticación diferenciadas por perfil de usuario.
- Control de ancho de banda.
- Registro de eventos y trazabilidad de accesos.
- Separación lógica entre red institucional y red de invitados.

Implementación y entregables

El contratista deberá:

- Realizar estudio técnico de cobertura (site survey predictivo y/o validación en campo).
- Determinar ubicación óptima de puntos de acceso.
- Instalar y configurar la totalidad de los equipos.
- Integrar la solución con la infraestructura de red cableada existente.
- Entregar planos de cobertura y memoria técnica.
- Entregar credenciales administrativas bajo acta.
- Realizar pruebas de funcionamiento y acta de recibo a satisfacción.
- Capacitar al personal designado por la Entidad.