ANEXO 1 – FICHA TÉCNICA

OBJETO:

"PRESTAR EL SERVICIO INTEGRAL DE TELECOMUNICACIONES, SEGURIDAD DIGITAL, SOPORTE TÉCNICO Y ADQUISICIÓN E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE NETWORKING INALAMBRICO PARA EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA DANE DE ACUERDO CON LOS REQUERIMIENTOS TÉCNICOS DEFINIDOS"

RESUMEN DEL PROCESO

NECESIDADES A SATISFACER	Unidad de medida	Cantidad
1. CONECTIVIDAD SEDES DANE A NIVEL NACIONAL		
ENLACES DEDICADOS PUNTO A PUNTO SEDES DANE	Unidad	**31**
ENLACES SATELITALES PUNTO A PUNTO SEDES DANE	Unidad	**4**
SEGURIDAD INFORMÁTICA	Unidad	**6**
2. ENLACES DEDICADOS PUNTO A PUNTO CENTROS OPERATIVOS MUNICIPALES	Unidad	**115**
3. PLANES DE DATOS PARA DISPOSITIVOS MÓVILES	Unidad	**8.986**
4. SOLUCIÓN DE RED INALAMBRICA	Unidad	**300** (APS) **2** (CONTROLADORA)

1. CONECTIVIDAD SEDES DANE A NIVEL NACIONAL

1.1 ENLACES DEDICADOS PUNTO A PUNTO SEDES DANE

Los enlaces a suministrar se listan a continuación y se presentan las características solicitadas para cada uno de ellos:

ID	Sede	Dirección	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	BW SD-WAN	Tiempo Meses	Estimado Usuarios Concurrentes	Zona
1	BOGOTA - DANE CENTRAL	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	Enlaces de Conectividad Terrestre	Enlaces Dedicados a Internet	1Gbps	1Gbps	1:1	SE REALIZA SOBRE EL MPLS DE LA SEDE	9	2224	Zona 1

ID	Sede	Dirección	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	BW SD-WAN	Tiempo Meses	Estimado Usuarios Concurrentes	Zona
2	BOGOTA - DANE CENTRAL	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	1Gbps	1Gbps	1:1	SE REALIZA SOBRE EL INTERNET DE LA SEDE	9		
3	BOGOTA - CASA ESMERALDA	Cr 59A No 44A-30 Bogotá	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	60Mbps	60Mbps	1:1	60Mbps	9	100	
4	BOGOTA - ALAMOS	Calle 64G No. 92 - 56 / Álamos Industrial	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	128Mbps	128Mbps	1:1	128Mbps	9	360	Zona 1
5	TUNJA	Carrera 11 No. 20-41 Piso 4	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	46Mbps	46Mbps	1:1	46Mbps	9	73	Zona 1
6	NEIVA	Calle 18 No. 7-75 Barrio Quirinal	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	26Mbps	26Mbps	1:1	26Mbps	9	68	Zona 1
7	VILLAVICENCIO	Carrera 43D No. 16-06 Barrio El Buque	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	26Mbps	26Mbps	1:1	26Mbps	9	73	Zona 1
8	FLORENCIA	Calle 24 No. 4A - 49, Barrio la Libertad	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	26Mbps	26Mbps	1:1	26Mbps	9	33	Zona 2
9	YOPAL	Transversal 18 No. 7-05 Piso 4 Centro	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	26Mbps	26Mbps	1:1	26Mbps	9	22	Zona 2
10	BARRANQUILLA	Calle 72 No. 58 - 65 Piso 1 y 2, ED. CENTRO	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	164	Zona 1
11	CARTAGENA	Bosque Sector San Isidro, Transversal 54 No. 28 – 25 Edificio Movisol 4 piso	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	66	Zona 1
12	SINCELEJO	Calle 25 No. 24-64 Piso 3	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	32	Zona 2

ID	Sede	Dirección	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	BW SD-WAN	Tiempo Meses	Estimado Usuarios Concurrentes	Zona
13	SANTA MARTA	Calle 17A No. 9-104 Barrio el pueblito	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	161	Zona 1
14	RIOHACHA	Carrera 11 No. 13 -39 Barrio Libertador	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	32	Zona 3
15	VALLEDUPAR	Carrera 6 No. 15-32 Plaza Alfonso López	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	53	Zona 1
16	SAN ANDRES	Avenida Francisco Newball No. 9- 184 Sector Los Almendros	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	10Mbps	9	84	Zona2
17	CUCUTA	Calle 13 No. 5 - 09 Centro Primer Piso	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	118	Zona 2
18	BUCARAMANGA	Calle 22 No 24 - 54 Barrio Alarcón	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	42Mbps	42Mbps	1:1	42Mbps	9	210	Zona 1
19	ARAUCA	Calle 21 No.15 - 13 Barrio Santa Teresita	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	4Mbps	4Mbps	1:1	4Mbps	9	65	Zona 3
20	CALI	Avenida 6B Norte No. 26N – 55 Barrio Santa Mónica Residencial	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	223	Zona 1
21	PASTO	Calle 20A No. 28-19 piso 2 al 5	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	16Mbps	16Mbps	1:1	16Mbps	9	117	Zona 2
22	POPAYAN	Carrera 9 No. 8N-20 Barrio Belalcázar	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	16Mbps	16Mbps	1:1	16Mbps	9	52	Zona 2
23	MANIZALES	Calle 77 No. 21-69 Barrio Milán	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	113	Zona 1

ID	Sede	Dirección	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	BW SD-WAN	Tiempo Meses	Estimado Usuarios Concurrentes	Zona
24	ARMENIA	CALLE 20 A No. 15-16 Edificio Torre Yanuba Piso 3	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	36Mbps	36Mbps	1:1	36Mbps	9	46	Zona 1
25	PEREIRA	Calle 19 No. 9-75, Edificio Palacio Nacional. Piso 3	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	16Mbps	16Mbps	1:1	16Mbps	9	88	Zona 1
26	MEDELLIN	Calle 44 No. 65 - 23 Barrio San Joaquín	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	100Mbps	100Mbps	1:1	100Mbps	9	333	Zona 1
27	MONTERIA	Calle 32 No. 10-44 Centro La Ceiba	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	16Mbps	16Mbps	1:1	16Mbps	9	125	Zona 1
28	QUIBDO	Carrera 9 No. 25-68 Barrio Alameda Reyes Edificio Cínica Citará Oral	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	14Mbps	14Mbps	1:1	14Mbps	9	18	Zona 2
29	IBAGUE	Calle 11 No. 3-32 Edificio Banco de la República Piso 7	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	26Mbps	26Mbps	1:1	26Mbps	9	61	Zona 1
30	BOGOTA, CORABASTOS	Avenida Carrera 80 No. 2 54, CORABASTOS, BODEGA 47 LOCAL 0501	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	10Mbps	9	20	Zona 1
31	SAN JOSE DEL GUAVIARE	Calle 5A No. 27 - 16, barrio 20 de Julio	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	4Mbps	4Mbps	1:1	4Mbps	9	10	Zona 3

GENERALIDADES	Se requiere una solución de enlaces de conectividad que comunique las sedes a nivel nacional del DANE con la sede del nivel central en la ciudad de Bogotá. Su objetivo es transmisión de datos y/o acceso a Internet centralizado a través del canal de internet de la sede principal. Los enlaces dedicados podrán ser implementados en diferentes tecnologías de Red de última milla, para los cuales se deberán priorizar los medios terrestres como fibra óptica, radio enlace o cobre donde sea necesaria su utilización. El Proveedor debe suministrar el servicio utilizando la mejor tecnología disponible de manera que le permita cumplir los ANS y las características técnicas definidas en los requerimientos técnicos. • Se requiere una red MPLS que conecte a todas las sedes regionales con la sede principal y viceversa. • Se requieren canales sin reúso, incluyendo elementos y configuraciones que permitan su operación las 24 horas del día.

	• Se requiere un canal de Internet para instalar en la sede principal del DANE en la ciudad de Bogotá mínimo de 1Gbps. • Se requiere un canal de MPLS para instalar en la sede principal del DANE en la ciudad de Bogotá mínimo de 1Gbps. • La disponibilidad de los canales de internet en la sede principal del DANE debe ser de >=99.9% garantizando que sean canales con alta disponibilidad y con doble equipo CPE. • La disponibilidad del punto de concentración de la red MPLS en la sede principal del DANE debe ser de >=99.9% garantizando que sean canales con alta disponibilidad y con doble equipo CPE. • La conectividad física para el total de sedes remotas y sede principal del DANE deberá estar provista de elementos para garantizar la operatividad del servicio, es decir implementar doble enlace de conectividad en las sedes con SDWAN, doble enlace de conectividad a en la sede principal del DANE, haciendo uso de canales con medio de transporte en fibra óptica y/o radioenlaces licenciados. Para brindar al DANE el mayor nivel de eficiencia y disponibilidad en la continuidad del servicio y en la calidad de la comunicación. • En caso de instalación de radio enlaces, estos deberán ser radio enlaces licenciados, no se aceptan radio enlaces no licenciados. • Todos los servicios de enlaces de conectividad deberán prestarse sin reúso. • Para los enlaces de Internet dedicado, el proveedor debe garantizar acceso internacional mínimo el 100% del ancho de banda del enlace contratado. • El oferente debe adjuntar una carta suscrita por el representante legal del proveedor de comunicaciones donde se garantice una cobertura con red propia de mínimo el 80% para los enlaces MPLS principales (última milla principal) de la red del DANE. • El oferente debe adjuntar una carta suscrita por el representante legal del proveedor de comunicaciones donde se garantice que mínimo el 90% de los enlaces MPLS terrestres principales se entregan con última milla en fibra óptica. • El oferente deberá brindar el servicio de administración de registros DNS que la Entidad requiera.
MODIFICACIÓN DE ENLACES	La Entidad podrá solicitar el traslado de los enlaces en situaciones en las que las sedes experimenten un cambio de ubicación. En tales circunstancias, el proveedor deberá atender el requerimiento procediendo a instalar el canal correspondiente en la nueva ubicación. Asimismo, en el caso de que la Entidad necesite ajustar el ancho de banda de alguno de los canales, el proveedor deberá atender dicha solicitud conforme a lo definido en Acuerdos de Niveles de Servicio (ANS) relacionados con la elasticidad.
DIRECCIONAMIENTO PUBLICO	Para el canal de internet el proveedor deberá suministrar 1 segmento (510 direcciones utilizables - prefijo /23) de direcciones IPv4, públicas que puedan ser utilizadas por la Entidad para publicar sus servicios. El proveedor debe adelantar las acciones técnicas necesarias para garantizar el correcto tráfico de IPv6 por medio de estos enlaces. Estas acciones estarán encaminadas a apoyar a la Entidad para habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de que hacen parte de la contratación y que soporte tal direccionamiento. El proveedor deberá apoyar el proceso de validación de la funcionalidad de los siguientes servicios y aplicaciones de la Entidad sobre IPv4 e IPv6: o Servicio de Resolución de Nombres (DNS) o Servicio de Asignación Dinámica de Direcciones IP (DHCP) o Directorio Activo

	○ Servicios WEB ○ Servidores de Monitoreo ○ Validación del Servicio de Correo Electrónico ○ Validación del Servicio de la Central Telefónica ○ Servicio de respaldo ○ Servicio de Comunicaciones Unificadas ○ Servicios VPN ○ Integración entre Sistemas de Información, Sistemas de Almacenamiento, Servicios de administración de red. Apoyar el proceso de activación de las políticas de seguridad de IPv4 y/o IPv6 en los equipos de seguridad y comunicaciones que hagan parte del contrato. Apoyar la configuración y puesta en funcionamiento de la conectividad integral en IPv4 e IPv6 desde el interior de las redes LAN, hacia el exterior de las redes WAN de todos los equipos y servicios que hacen parte del contrato a fin de garantizar que la Entidad puedan generar tráfico normalmente. Las direcciones IP no deben tener ningún tipo de restricción o reporte en listas negras. El Proveedor debe garantizar que todos los componentes de los servicios de conectividad soportan y son compatibles tanto en IPv4 e IPv6. La Entidad posee su propio direccionamiento IPv6, por lo tanto se requiere que el proveedor realice la configuración de última milla tanto del lado de la Entidad como del lado del Proveedor garantizando que los servicios a publicar funcionen correctamente y sea posible la generación de tráfico IPv6 sobre estos servicios. El Proveedor del servicio debe acogerse a las políticas de direccionamiento y transición en modo Doble Pila (Dual Stack) de IPv6.
SD-WAN	SD-WAN (Software Defined Wide Area Network) es una herramienta de control dinámico de múltiples canales de ancho de banda que permite gestionar y balancear de manera flexible el envío de paquetes, optimizar el enrutamiento a nivel de aplicación, ordenándolo de acuerdo con reglas, políticas y parámetros definidos por la Entidad, permitiendo la clasificación, análisis y control. La conectividad SD-WAN debe contar con los anchos de banda especificados en el listado de sedes presentado anteriormente. El Proveedor debe suministrar el servicio solicitado proporcionando e instalando los equipos necesarios que le permitan cumplir con las funcionalidades, características técnicas y los ANS definidos en esta ficha. La entidad requiere el servicio SD-WAN para cada sede con las siguientes características: • Los equipos SD-WAN deben ser nuevos. • El proveedor debe contar con conexión directa al NAP Colombia. • Los Canales de Datos y de Internet deben estar configurados en modo Activo – Activo. • La arquitectura de la conexión deberá estar en un enlace de datos y un enlace a internet, sobre los cuales se configure la SD-WAN, y el ancho de banda se pueda aprovechar al 100% siempre, si hay una caída en alguno de los enlaces no habrá indisponibilidad al estar en esquema activo-activo.

	• Para la sede central del DANE el servicio de SD-WAN se realizará con el canal a internet principal de la sede. • La solución SD-WAN se debe integrar de forma nativa con el servicio de Firewall de la Entidad. • Solución SD-WAN con última milla redundante y medios diferentes con balanceo de cargas en caso de falla en estado activo-activo. • Control de camino incluido en el equipo SD-WAN, sin depender de una controladora centralizada. • Distribución de tráfico inteligente basada en aplicación, direcciones IP de origen y destino, usuarios o grupos de usuarios. • Monitoreo activo de estado de salud de los enlaces, basado en al menos retardo, jitter y pérdida de paquetes. Este monitoreo debe poderse hacer al menos usando ping y HTTP. • Monitoreo pasivo de los enlaces, con base en el tráfico real de los usuarios. • Failover automático en caso de falla o degradación de uno de los enlaces. • Forward Error Correction (FEC), para corrección de errores en enlaces ruidosos. • Debe ser capaz de proveer una arquitectura de Auto Discovery VPN - ADVPN donde sea posible la integración con el Firewall de Nueva Generación de Nube Pública de la entidad y con las diferentes sedes • La solución debe tener soporte de VPNs IPSec sitio a sitio y cliente – sitio con algoritmos de cifrado AES256, AES192; algoritmos de integridad SHA-1, SHA256, SHA-384 y SHA-512; grupos de Diffie-Hellman 1, 2, 5, 14, 21 y 32. • La solución debe tener capacidad de integrarse con Servidores de Autenticación: RADIUS, LDAP, TACACS+, POP3, SSO y RSA ACE. • La solución debe permitir control de aplicaciones basado en categorías (por lo menos 15), incluyendo, pero no limitado a: tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe permitir la diferenciación de aplicaciones proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • La solución debe tener un listado de al menos 4000 aplicaciones ya definidas por el fabricante. • La solución debe permitir inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados. • Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv4 e IPv6. • La solución no debe estar licenciada con base en el ancho de banda contratado. • La solución debe brindar funcionalidad de Filtrado Web, Filtrado DNS, IPS e inspección SSL para IPv4 e IPv6 para la protección del tráfico de usuarios por el canal de Internet Local. • La solución debe brindar funcionalidad de antimalware de perímetro con integración nativa con la plataforma de Sandbox del SOC de la entidad, para la remisión de archivos sospechosos con el fin de ser analizados y detectar ataques de día cero. • Debe permitir la configuración de políticas de QoS en la capa 7, asociadas porcentualmente al ancho de banda de la interfaz SD-WAN

	• Debe permitir la configuración de políticas de QoS en valores donde el máximo corresponda a la totalidad del ancho de banda disponible en el equipo.
	• La solución debe integrarse de manera nativa con la plataforma de reportes de seguridad de la entidad, así como con el SIEM del SOC de la entidad.
	• Debe permitir la consulta vía SNMPv2 / v3 referente a los siguientes datos:
	  ○ Estado actual de los enlaces SD-WAN
	  ○ Latencia
	  ○ Jitter
	  ○ Packet Loss
	  ○ Paquetes enviados / paquetes recibidos
	  ○ Link Bandwitdh
	  ○ VRF asociado
	• Debe posibilitar la distribución de peso en cada uno de los enlaces que componen el SD-WAN, a criterio del administrador, de forma que el algoritmo de equilibrio utilizado pueda basarse en:
	  ○ Número de sesiones,
	  ○ Volumen de tráfico,
	  ○ IP de origen y destino
	  ○ desbordamiento de Enlace (Spillover)
	• Debe contar con la capacidad de balanceo de tráfico por paquete.
	• Debe ser capaz de admitir una arquitectura de transporte multidifusión IPv4 e IPv6 a través de túneles VPN IPSEC construidos en ADVPN.
	• Debe contar con soporte de IPv6 en overlay y underlay de SD-WAN.
	• Debe tener la capacidad de autenticar a los usuarios para la administración del equipo a través de la base de datos:
	  ○ Local
	  ○ Integrada en el servidor TACACS +
	  ○ Integrada en el servidor LDAP
	  ○ Alternativamente debe soportar base de datos centralizada propia, donde toda la arquitectura SD-WAN converge a ella
	• La Alta Disponibilidad proporcionada por La funcionalidad de SD-WAN, deberá cumplir los siguientes criterios:
	  ○ Soporte Balanceo Activo - Activo
	  ○ Soporte Balanceo Activo - Pasivo
	  ○ Soporte Balanceo de hasta 4 peers
	  ○ Soporte Balanceo Distribuido Geográficamente
	• La funcionalidad SD-WAN debe ofrecer solución de problemas en la consola de línea de comandos o gráfica, donde sea posible:
	  ○ Ejecutar Packet sniffer del tráfico interesante, filtrando por: IP y Puerto
	  ○ Realizar depuración detallada de las fases de negociación VPN
	• La funcionalidad SD-WAN debe ofrecer una visualización gráfica de:
	  ○ Aplicaciones más utilizadas con su ancho de banda
	  ○ Shaping de tráfico SD-WAN
	  ○ IP de destino más utilizados con su número de sesiones y ancho de banda asociados
	• La funcionalidad SD-WAN debe admitir la marcación de paquetes DSCP en las definiciones y reglas para el tráfico SD-WAN.

LATENCIA	Mide el tiempo promedio que tarda un paquete IP en ir y volver entre los siguientes puntos:

	- Desde el router de la Entidad hasta el NAP Colombia. La medición la hace el Proveedor durante todo el tiempo de servicio. Los resultados de las muestras son mantenidas por el Proveedor para que puedan ser consultadas por la Entidad Compradora durante la duración del servicio con el fin de verificar la latencia promedio que permita garantizar el cumplimiento de este indicador. Latencia: **máximo 40ms**
DISPONIBILIDAD EXIGIDA	La disponibilidad se mide usando la siguiente ecuación: $\left(1 - \frac{Número\ total\ de\ minutos\ en\ que\ el\ servico\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ contratados\ x\ 24\ horas\ x\ 60\ minutos}\right) x\ 100\%$ La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio de intercambio de datos sobre el enlace no está disponible, dividido en el número total de minutos en el mes facturado. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. Cada sede con SDWAN deberá incluir un enlace MPLS y un enlace de Internet, cada uno de estos enlaces no pueden compartir la misma última milla, ni mismo nodo del proveedor. La medición se hace teniendo en cuenta el conjunto de enlaces que se tendrían en la sede, es decir, la medición es por sede, en donde cada sede debe cumplir con el valor exigido en el ANS. **Disponibilidad exigida >=99.9% mensual** **Penalidad por no conformidad - Descuento en facturación** • 99.6%<=Disponibilidad<99.9%: 10% de descuento sobre el costo este servicio. • 99.3%<=Disponibilidad<99.6%: 20% de descuento sobre el costo este servicio. • 99%<=Disponibilidad<99.3%: 50% de descuento sobre el costo este servicio. • Disponibilidad<99%: 100% de descuento sobre el costo este servicio.
RTO	El RTO por sus siglas en inglés es Recovery Time Objective o en español Tiempo Objetivo de Recuperación. El RTO es el tiempo máximo que el enlace puede estar fuera de servicio una vez se ha producido una Interrupción. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad

	verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. En los casos en que la interrupción sea en la herramienta de monitoreo y no en el servicio; no se contabilizará la interrupción como parte del tiempo máximo que el servicio puede estar fuera de servicio. **RTO <= 8 minutos** **Penalidad por no conformidad - Descuento en facturación** • 8 min<RTO<=15 min: 10% de descuento sobre el costo total de este servicio. • 15 min<RTO<=25 min: 20% de descuento sobre el costo total de este servicio. • 25 min<RTO<=45 min: 50% de descuento sobre el costo total de este servicio. • 45 min<RTO: 100% de descuento sobre el costo total de este servicio.
INTERRUPCIONES MÁXIMAS	El ANS Interrupciones máximas hace referencia a el número máximo de Interrupciones durante el mes facturado. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma por sede teniendo en cuenta el conjunto de enlaces allí instalados, es decir, cada sede debe cumplir con el valor exigido en el ANS. **Interrupciones máximas en un mes: 1 interrupciones** **Penalidad por no conformidad - Descuento en facturación** • 2 interrupciones: 20% de descuento sobre el costo de este servicio. • 3 interrupciones: 50% de descuento sobre el costo de este servicio. • >4 Interrupciones: 100% de descuento sobre el costo de este servicio.
MTBF	El MTBF por sus siglas en inglés es Mean Time Between Failures o en español Tiempo Medio Entre Fallas. El MTBF es un indicador de confiabilidad definido como el promedio aritmético acumulado del tiempo entre Fallas asumiendo que el enlace se recupera de forma inmediata cuando se produce la Falla. Nota aclaratoria: El supuesto: “asumiendo que el servicio se recupera de forma inmediata” hace referencia a la forma en que se medirá en tiempo entre fallas y no a que necesariamente haya una recuperación instantánea de una falla.

	Una falla se define como una degradación del servicio de conectividad con respecto a las condiciones pactadas en al Acuerdo Marco de Precios La medición la hace el Proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. La información mantenida por el Proveedor le debe permitir a la Entidad verificar el MTBF acumulado en cualquier momento durante la prestación del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. Nota aclaratoria: Una Falla es diferente a una Interrupción. La Falla está asociada a la confiabilidad del servicio y la Interrupción está asociada a la disponibilidad del servicio. **MTBF =720 horas** • 650 horas < MTBF = 720 horas: 10% de descuento sobre el costo total de este servicio. • 500 horas < MTBF <= 650 horas: 20% de descuento sobre el costo total de este servicio. • 400 horas < MTBF <= 500 horas: 50% de descuento sobre el costo total de este servicio. • MTBF < 400 horas: 100% de descuento sobre el costo total de este servicio.
ANCHO DE BANDA	El ancho de banda corresponde al rango de frecuencias que ocupan los datos transmitidos por el enlace sin que se presente distorsión o pérdida de información. La medición la debe hacer el Proveedor una vez lo solicite el DANE por el tiempo y con la frecuencia que la Entidad lo requiera. Los resultados de la medición deben ser mantenidos por el Proveedor para que puedan ser consultados por la Entidad durante la duración del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Ancho de banda** Debe ser igual o superior al ancho de banda contratado **Penalidad por no conformidad - Descuento en facturación** • Si se evidencia una reducción del 10% sobre el ancho de banda contratado: 40% de descuento sobre el costo del servicio • Si se evidencia una reducción del 20% sobre el ancho de banda contratado: 50% de descuento sobre el costo del servicio • Si se evidencia una reducción >= 30% sobre el ancho de banda contratado: 100% de descuento sobre el costo del servicio
CALIDAD Y OPORTUNIDAD EN LOS REPORTES ENTREGADOS	El Proveedor debe garantizar la calidad de la información que contienen los reportes que entrega a la Entidad. Con el fin de garantizar la calidad de los reportes se define el número máximo de devoluciones en que puede incurrir el Proveedor sin que se generen penalizaciones para cada nivel de servicio. Adicionalmente, se establecen las

	penalidades por no conformidad que se le harán al Proveedor cuando supera el número máximo de devoluciones. **Devoluciones máximas por cada reporte** <= 2 devoluciones de un mismo reporte **Penalidad por no conformidad - Descuento en facturación** • 3 devoluciones del mismo reporte: 10% • 4 devoluciones del mismo reporte: 20% • 5 devoluciones del mismo reporte: 50% • 6 devoluciones del mismo reporte: 100%
ELASTICIDAD	**Crecimiento definitivo** Ampliaciones definitivas en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. Una ampliación definitiva tiene una duración correspondiente al tiempo restante de servicio. Capacidad de crecimiento: Hasta el 100% sin cambio de equipos. **Crecimiento temporal** Ampliaciones en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. • Capacidad de crecimiento: Hasta el 100% sin cambio de equipos **Duración del crecimiento** • Mínima (días): Entre 7 días calendario hasta 30 días calendario Máxima (mensual): 60 días calendario
TIEMPO DE APROVISIONAMIENTO DE CRECIMIENTOS CONTEMPLADOS EN EL NIVEL DE ELASTICIDAD CONTRATADO	El crecimiento de los enlaces está dado por las características de elasticidad definidas en esta ficha. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Elasticidad alta** <= a 16 horas continuas **Penalidad por no conformidad - Descuento en facturación** • 2 horas continuas de retraso: 10% de descuento sobre el costo este servicio. • 4 horas continuas de retraso: 20% de descuento sobre el costo este servicio. • 6 horas continuas de retraso: 50% de descuento sobre el costo este servicio. • 8 horas continuas de retraso: 100% de descuento sobre el costo este servicio.
EFECTIVIDAD EN RESOLUCIÓN DE INCIDENTES/SOLICITUDES	Aplicable para: • Solicitudes de cambios • Cambios en configuraciones • Habilitación de VPN. • Resolución de inquietudes • Entrega reportes e información. • Solución de incidentes

	La efectividad de resolución de solicitudes mide el tiempo máximo de solución de las solicitudes realizadas a la mesa de ayuda del Proveedor según su nivel de prioridad. El reloj que mide la efectividad de resolución comienza a contabilizar el tiempo desde el momento en que el ticket es registrado en la mesa de ayuda hasta que el Proveedor da una respuesta y soluciona el problema. Zona 1: Prioridad 1: Efectividad de resolución <=4 horas Prioridad 2: Efectividad de resolución <= 18 horas Prioridad 3: Efectividad de resolución <= 64 horas Zona 2: Prioridad 1: Efectividad de resolución <= 8 horas Prioridad 2: Efectividad de resolución <= 32 horas Prioridad 3: Efectividad de resolución <= 88 horas Zona 3 y 4: Prioridad 1: Efectividad de resolución <= 20 horas Prioridad 2: Efectividad de resolución <= 48 horas Prioridad 3: Efectividad de resolución <= 112 horas Un incidente puede causar: Interrupción no planeada del servicio. Reducción de la calidad del mismo. Falla de un servidor que todavía no ha impactado un servicio. Prioridad 1: Son los casos por eventos cuando afecta al core del negocio, si este no se llegase a solucionar con reinicio, se maneja como IM (Incidente Mayor). Prioridad 2: Cuando no se ha afectado la disponibilidad del servicio total, pero hay un alto riesgo Prioridad 3: Afectación de un servidor no core. Un server caído de un ambiente de pruebas.
HARDWARE Y SOFTWARE	El Proveedor debe garantizar toda la conectividad física y lógica requerida para la puesta en funcionamiento de los servicios y conectividad contratada. La conectividad física hace referencia a todos los elementos de hardware necesarios para proveer el servicio. El DANE dispone de las condiciones de infraestructura para la entrega del servicio, tales como: energía regulada, sistema de puesta a tierra, rack y espacios de comunicaciones para instalar equipos de telecomunicaciones y condiciones ambientales óptimas para la temperatura de los equipos, esto en el caso que los servicios contratados así lo requieran. La conectividad lógica hace referencia a todos los elementos de software necesarios y su respectiva configuración para proveer el servicio. El proveedor deberá implementar su solución tecnológica para que la misma se integre con las plataformas tecnológicas que posee la Entidad.

NAP COLOMBIA	El ISP (Internet Service Provider) debe incluir conexión al NAP Colombia garantizando el 100% del ancho de banda contratado por parte de la Entidad compradora, garantizando que el tráfico de datos que tiene origen y destino en el territorio nacional no transite por enlaces internacionales y en conformidad a lo establecido en la Res. CRC 5078 de 2016 "Indicadores de Calidad" Res. 5050 "compilada de las resoluciones de carácter general" y todas aquellas que adicionen, modifiquen o sustituyan. El proponente deberá presentar una certificación en donde demuestre que hace parte del NAP Colombia de forma directa y que cuenta con un acceso en fibra óptica.
ENLACES DE SALIDA INTERNACIONAL A INTERNET	El Proveedor debe contar con al menos dos salidas a Internet internacional (medios físicos de salida diferentes) que deben ser configuradas para permitir el direccionamiento en compatibilidad IPv4 e IPv6. El Proveedor debe ofrecer para las salidas internacionales a internet, enlaces de comunicaciones de alta disponibilidad capaces de soportar el tráfico y compatibilidad de IPv4 e IPv6 simultáneo sin inconvenientes de ancho de banda. Esta condición podrá ser cumplida ya sea de manera directa o a través del proveedor con el que tenga el convenio correspondiente. El proponente deberá contar con salida internación a través de su propio cable submarino y contar con redundancia a través de mínimo otros 3 operadores. Se deberá entregar certificado en donde se conste que el proveedor cuenta con su propio cable submarino. El oferente deberá presentar la carta en donde se certifique que cuenta con su propio cable submarino.
REGISTRO TIC	El Proveedor para la prestación de los servicios de telecomunicaciones solicitados, deberá contar con el Registro TIC emitido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones el cual lo acredita como Proveedor de Redes y Servicios de Telecomunicaciones en el territorio nacional. El Registro TIC deberá estar vigente durante toda la ejecución del contrato.
AISLAMIENTO DE RED	El Proveedor debe garantizar que el servicio de conectividad admite controles de aislamiento de red para tráfico entrante y saliente a través de métodos a nivel de capa 2 o 3. El Proveedor debe articular cualquier restricción, condición o requisito de red, como la traducción de dirección de red (NAT), la superposición de direcciones IP y controles de latencia para los procesos de traducción NAT.
SERVICIO DE SOPORTE TÉCNICO	El Proveedor debe tener la capacidad de brindar servicio de soporte técnico remoto y/o en sitio para los servicios contratados por la Entidad. El Proveedor debe brindar soporte en sitio para evaluar y solucionar fallas e Interrupciones que se presenten en los servicios contratados por la Entidad. El soporte será en sitio sólo en los casos en que no sea posible resolver el problema de forma remota. El servicio en sitio no significa costos adicionales para el DANE. Adicionalmente, el Proveedor debe brindar soporte remoto a nivel nacional a través de los siguientes canales: • Línea de atención telefónica gratuita con cobertura nacional. • Plataforma web para registro y monitoreo de tiquetes.

	• Correo electrónico. • Chat. El Proveedor debe garantizar que cuenta con un servicio de mesa de ayuda el cual deberá operar en instalaciones a cargo del proveedor. El Proveedor debe garantizar que exista un tiquete por cada reporte de Falla o Interrupción que haga el DANE. Los canales de soporte deben estar disponibles 7x24 durante el tiempo de ejecución del contrato. El grupo de soporte del Proveedor debe garantizar que los tickets: • Sean registrados, clasificados y asignados según su criticidad. • Sean resueltos en los tiempos acordados en los ANS. • Tengan un seguimiento adecuado. • Cumplan con esquemas de escalamiento definidos. Deben ser documentados con las respectivas evidencias y en caso de requerir atención en sitio anexar registros fotográficos donde se observe Georreferenciación, fecha y hora donde ocurrió el evento. El proveedor debe garantizar que cuenta con la especialidad de SD_WAN del fabricante de la solución, esta certificación debe emitirla el fabricante, estar dirigida a la entidad e indicar el número del proceso.
SERVICIO DE SOPORTE TÉCNICO - EFECTIVIDAD EN LA ATENCIÓN DE LOS CANALES	El Proveedor debe garantizar tiempos de efectividad en la atención para cada canal como se detalla a continuación: • Línea telefónica nacional gratuita: <= 2 minutos. • Plataforma web para registro y monitoreo de tiquetes: <= 2 minutos. • Correo electrónico: <= 5 minutos. • Chat: <= 3 minutos.
SERVICIO DE SOPORTE TÉCNICO - NIVELES DE ATENCIÓN Y ESCALAMIENTO	El Proveedor debe Incluir el servicio de soporte técnico para el manejo de niveles 1 y 2 de soporte. Adicionalmente, el servicio de soporte técnico suministrado por el Proveedor debe gestionar escalamientos a nivel 3 o superior cuando corresponda. El proveedor del servicio de conectividad al inicio de la ejecución del contrato deberá entregar un documento en el que indique el nivel de escalamiento (Nombre del profesional, cargo, correo electrónico y número de celular de contacto) con al menos tres (3) profesionales asignados por el proveedor que permitan, elevar los requerimientos en caso de la no atención satisfactoria de las solicitudes. los perfiles asignados deberán ser al menos en el nivel 1. tecnólogo, y en los niveles 2 y 3 profesionales con vinculación con el proponente.
SERVICIO DE SOPORTE TÉCNICO - PRIORIZACIÓN DE TICKETS	Los tiquetes deben ser clasificados y atendidos según su nivel de criticidad. Los criterios para llevar a cabo dicha clasificación son los siguientes: **Prioridad 1:** Emergencia - Una Falla que afecta un proceso critico de la Entidad.

	Prioridad 2: Degradación en el servicio - Una Falla que afecta el desempeño o confiabilidad de un proceso de la Entidad. **Prioridad 3:** Inquietud o solicitud - Solicitudes de soporte menores o de información que no tienen impacto en los procesos de la Entidad. Incluye: Solicitudes de cambios, cambios en configuraciones, habilitación de VPN, resolución de inquietudes y entrega de información.
SERVICIO DE SOPORTE TÉCNICO - REPORTES DE GESTIÓN	El Proveedor debe entregar reportes mensuales de mesa de ayuda al supervisor del contrato, que permitan monitorear las siguientes variables: • Número de incidentes reportados según nivel de criticidad. • Número de incidentes resueltos que incluya el tiempo promedio de resolución según nivel de criticidad. • Análisis de causa raíz para incidentes relacionados. • Propuestas de mejora continua para los servicios contratados. • 2 variables más que defina la Entidad Compradora. La Entidad Compradora definirá las variables teniendo en cuenta que puedan ser soportados por la herramienta de monitoreo del Proveedor. El Proveedor debe entregar un reporte consolidado de mesa de ayuda una vez concluya el servicio de conectividad contratado. El proveedor debe contar con una plataforma que le permita al DANE visualizar consumo de canales en tiempo real y enviar reportes automáticos mensuales.
OBRA CIVIL	El servicio suministrado por el Proveedor incluye los costos y responsabilidades que significa adecuar la obra civil desde sus instalaciones (las del Proveedor) hasta cada uno de los puntos indicados donde se requiere el servicio. El Proveedor debe incluir la solución de última milla por el medio de transmisión adecuado para cumplir con los requerimientos de la Entidad Compradora y que están alineados con las condiciones y ANS definidos para el servicio. En caso de que se requiera y de ser necesario adelantar una obra civil, en las instalaciones de la Entidad o alguna de sus sedes, esta se entiende como: canalización con tubería EMT (Electrical Metallic Tubing), que corresponde al tendido de cables instalados a través de canalizaciones que contienen los ductos que permiten el tendido, la protección y el mantenimiento de cables de red y también de cables de fibra óptica. Se debe contemplar la instalación, adecuación y señalización de cables o fibra sobre canaletas de las instalaciones de la Entidad. El Proveedor debe estimar el costo total de la obra civil desde la acometida hasta el punto donde la Entidad requiere el enlace e incluirlo en el valor de instalación. Los costos en que incurra el Proveedor por la obra civil desde sus instalaciones (las del Proveedor) hasta la acometida en las sedes de la Entidad son responsabilidad del Proveedor.
TIEMPOS DE INSTALACIÓN	Es el tiempo máximo que puede tardar el Proveedor en hacer las instalaciones sin incurrir en incumplimiento, los cuales se solicitan de la siguiente manera: <= **35 días calendario**

	El proveedor entrante debe garantizar una transición controlada con el proveedor actual, evitando que se presenten interrupciones en ninguno de los servicios que actualmente brinda la Entidad a los usuarios. En este sentido, el proveedor entrante deberá asumir todos los costos asociados con la continuidad actual del servicio durante el tiempo necesario para llevar a cabo sus propias instalaciones y configuraciones, de manera que la Entidad no experimente ninguna indisponibilidad del servicio, hasta que esté plenamente instalada la solución del nuevo operador a satisfacción de la Entidad.
ANÁLISIS DE VULNERABILIDADES	El proveedor deberá ejecutar de forma semestral un análisis de vulnerabilidades sobre la infraestructura utilizada para la prestación de los servicios de conectividad, incluyendo herramientas de gestión, plataformas de seguridad, equipos de borde, canales de acceso a internet y dispositivos de red entre otros. El análisis de vulnerabilidades deberá ejecutarse usando una herramienta licenciada, no open source, en esquema empresarial, que cuente con todas las actualizaciones que el fabricante de la herramienta disponga en términos de vulnerabilidades reportadas. Adicionalmente el Proveedor presentará el informe de las vulnerabilidades identificadas en las pruebas, según requerimiento de la entidad compradora, dentro de los siguientes 3 días hábiles posteriores a la solicitud. La prueba debe incluir como mínimo las IP, sistemas operativos y las vulnerabilidades detectadas de los sistemas escaneados. Este reporte deberá ser entregado al supervisor del contrato según su solicitud, incluyendo los requisitos establecidos**.**
NOTIFICACIÓN DE INCIDENTES Y ENTREGA DE INFORMES DE INDISPONIBILIDAD	El proveedor del servicio deberá notificar los incidentes mediante al menos dos medios diferentes de comunicaciones (SMS, Correo electrónico, aplicaciones como WhatsApp, entre otros) que la Entidad determine y al personal que defina. Adicionalmente la Entidad, podrá establecer o delimitar el tipo de incidentes desea que le sean reportados de acuerdo con el nivel de criticidad. El proveedor del servicio tendrá 24 horas a partir del momento de un incidente crítico para reportarle a la Entidad Compradora el informe detallado. En el cual deberá relacionar al menos motivo de la falla, tiempo de indisponibilidad, elementos y servicios afectados, mecanismo utilizado en la solución del incidente crítico y mecanismos de prevención del incidente a futuro. El proveedor del servicio determinará el formato utilizado para el informe siempre y cuando se cuente con al menos la información solicitada.
QoS y CoS	El Proveedor debe brindar en los enlaces QoS (Calidad de Servicio) y CoS (Clase de Servicio) en los casos en que la Entidad Compradora lo requiera.
PROTOCOLO SNMP	El Proveedor debe garantizar que todos los equipos necesarios, tienen habilitado el protocolo SNMP para poder supervisar el funcionamiento de la red.
	El Proveedor debe proporcionar una plataforma de monitoreo y uso de tráfico en vivo en la cual se pueda consultar el estado de los canales y el uso de estos mediante un servicio web para lo cual el proveedor deberá entregar al menos 2 usuarios para el uso de la Entidad. La plataforma debe mantener los resultados del monitoreo con gráficas, históricos de meses anteriores y para el mes en curso en tiempo real (con un retraso menor

PLATAFORMA DE MONITOREO	a 5 minutos), para que puedan ser consultados por la Entidad Compradora en cualquier momento durante la duración del servicio. La retención de la información corresponderá a toda la vigencia del contrato y podrá ser entregada a la entidad, previa solicitud, una vez finalizado el servicio. Los indicadores a monitorear incluyen las variables asociadas a los ANS que especifica cada ficha de servicio.
REPORTE DE GESTIÓN	El Proveedor debe monitorear y entregar un reporte de gestión a la Entidad incluido los eventos, la capacidad, la seguridad y la utilización de los diferentes componentes de los servicios de conectividad suministrados. El reporte de gestión debe incluir los resultados del seguimiento hecho durante el mes de los indicadores que a continuación se listan: - Disponibilidad. - Número máximo de interrupciones. - RTO. - MTBF. - Latencia. - Ancho de banda. Adicionalmente, para los servicios de enlaces terrestres y satelitales el Proveedor debe monitorear las siguientes variables: - Tráfico de entrada. - Tráfico de salida. El reporte de gestión del servicio que entrega el Proveedor debe contener, además; información de uso de los componentes de infraestructura que componen el servicio (ejemplo: ancho de banda consumida en línea de tiempo durante el periodo, VPNs configuradas, tráfico en el administrador del ancho de banda y eventos reportados por el firewall). El criterio de evaluación de calidad de los reportes hace referencia a que incluya todo el contenido detallado anteriormente." El Proveedor debe entregar los reportes de gestión y calidad del servicio y de cada componente que lo constituye con una periodicidad igual a la frecuencia de facturación.
DESCUENTOS EN FACTURACIÓN	El valor máximo de los descuentos corresponde al 100% del valor del servicio facturado aun cuando la suma total de los descuentos supere 100%.
DAÑOS Y MAL FUNCIONAMIENTO DE EQUIPOS	El Proveedor 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.
MANTENIMIENTO	El Contratista es responsable del mantenimiento de los equipos y dispositivos entregados por su cuenta para el desarrollo del contrato, de esta forma es su responsabilidad realizar mantenimientos preventivos y correctivos con el fin de garantizar el cumplimiento de los acuerdos de nivel de servicio (ANS).

1.2 ENLACES SATELITALES PUNTO A PUNTO SEDES DANE

Los enlaces a suministrar se listan a continuación y se presentan las características de cada uno de ellos.

ID	Sede	Dirección	Categoría	Nombre del servicio	BW down	BW upload	Re-USO	Asimetría	BW SD-WAN	Tiempo Meses	Estimado Usuarios Concurrentes	Zona
1	MITU	CARRERA 14 N° 12 - 43 LOCAL 3 HOTEL JM	Enlaces de Conectividad Satelital	Enlace Punto a Punto Satelital SCPC	4Mbps	2Mbps	1:1	1:2	2Mbps	9	3	Zona 4
2	PUERTO CARREÑO	CARRERA 11 NO. 19-81/93 BARRIO LAS ACACIAS	Enlaces de Conectividad Satelital	Enlace Punto a Punto Satelital SCPC	4Mbps	2Mbps	1:1	1:2	2Mbps	9	35	Zona 4
3	LETICIA	Carrera 7 No. 6-104 Barrio Punto Brava	Enlaces de Conectividad Satelital	Enlace Punto a Punto Satelital SCPC	4Mbps	2Mbps	1:1	1:2	2Mbps	9	6	Zona 4
4	PUERTO INIRIDA	Calle 17 No. 13-36 Barrio los Libertadores	Enlaces de Conectividad Satelital	Enlace Punto a Punto Satelital SCPC	4Mbps	2Mbps	1:1	1:2	2Mbps	9	8	Zona 4

GENERALIDADES	Se requiere una solución de Enlaces de conectividad satelital que comunique las sedes indicadas en esta sección con la red MPLS de las sedes a nivel nacional y con la sede del nivel central en la ciudad de Bogotá. Su objetivo es transmisión de datos y/o acceso a Internet a través de un desbordamiento centralizado a través del canal de internet de la sede principal. Los enlaces solicitados para interconectar las sedes por medio de conexiones con tecnología satelital con portadora exclusiva para la entidad que permita interconectar con la red MPLS. Aunque el Proveedor debe suministrar el servicio utilizando la mejor tecnología disponible de manera que le permita cumplir los ANS y características técnicas definidas en los requerimientos técnicos. El proveedor deberá evaluar nuevas tecnologías que optimicen el servicio en estas zonas, las cuales se aceptaran para implementar la solución.
MODIFICACIÓN DE ENLACES	La Entidad podrá solicitar el traslado de los enlaces en situaciones en las que las sedes experimenten un cambio de ubicación. En tales circunstancias, el proveedor deberá atender el requerimiento procediendo a instalar el canal correspondiente en la nueva ubicación. Asimismo, en el caso de que la Entidad necesite ajustar el ancho de banda de alguno de los canales, el proveedor deberá atender dicha solicitud conforme a lo definido en Acuerdos de Niveles de Servicio (ANS) relacionados con la elasticidad.
SD-WAN	SD-WAN (Software Defined Wide Area Network) es una herramienta de control dinámico de múltiples canales de ancho de banda que permite gestionar y balancear de manera flexible el envío de paquetes, optimizar el enrutamiento a nivel de aplicación, ordenándolo de acuerdo con reglas, políticas y parámetros definidos por la Entidad, permitiendo la clasificación, análisis y control.

	La conectividad SD-WAN debe contar con los anchos de banda especificados en el listado de sedes presentado anteriormente. El Proveedor debe suministrar el servicio proporcionando e instalando los equipos necesarios que le permitan cumplir con las funcionalidades, características técnicas y los ANS definidos en esta ficha. La entidad requiere el servicio SD-WAN para cada sede con las siguientes características: • Los equipos SD-WAN deben ser nuevos. • El Proveedor debe contar con conexión directa al NAP Colombia. • Los Canales de Datos y de Internet deben estar configurados en modo Activo – Activo. • La arquitectura de la conexión deberá estar en un enlace de datos y un enlace a internet, sobre los cuales se configure la SD-WAN, y el ancho de banda se pueda aprovechar al 100% siempre, si hay una caída en alguno de los enlaces no habrá indisponibilidad al estar en esquema activo-activo. • Para la sede central del DANE el servicio de SD-WAN se realizará con el canal a internet principal de la sede. • La solución SD-WAN se debe integrar de forma nativa con el servicio de Firewall de la Entidad. • Solución SD-WAN con última milla redundante y medios diferentes con balanceo de cargas en caso de falla en estado activo-activo. • Control de camino incluido en el equipo SD-WAN, sin depender de una controladora centralizada. • Distribución de tráfico inteligente basada en aplicación, direcciones IP de origen y destino, usuarios o grupos de usuarios. • Monitoreo activo de estado de salud de los enlaces, basado en al menos retardo, jitter y pérdida de paquetes. Este monitoreo debe poderse hacer al menos usando ping y HTTP. • Monitoreo pasivo de los enlaces, con base en el tráfico real de los usuarios. • Failover automático en caso de falla o degradación de uno de los enlaces. • Forward Error Correction (FEC), para corrección de errores en enlaces ruidosos. • Debe ser capaz de proveer una arquitectura de Auto Discovery VPN - ADVPN donde sea posible la integración con el Firewall de Nueva Generación de Nube Pública de la entidad y con las diferentes sedes • La solución debe tener soporte de VPNs IPSec sitio a sitio y cliente – sitio con algoritmos de cifrado AES256, AES192; algoritmos de integridad SHA-1, SHA256, SHA-384 y SHA-512; grupos de Diffie-Hellman 1, 2, 5, 14, 21 y 32. • La solución debe tener capacidad de integrarse con Servidores de Autenticación: RADIUS, LDAP, TACACS+, POP3, SSO y RSA ACE. • La solución debe permitir control de aplicaciones basado en categorías (por lo menos 15), incluyendo, pero no limitado a: tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

	• La solución debe permitir la diferenciación de aplicaciones proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
	• La solución debe tener un listado de al menos 4000 aplicaciones ya definidas por el fabricante.
	• La solución debe permitir inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados.
	• Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv4 e IPv6.
	• La solución no debe estar licenciada con base en el ancho de banda contratado.
	• La solución debe brindar funcionalidad de Filtrado Web, Filtrado DNS, IPS e inspección SSL para IPv4 e IPv6 para la protección del tráfico de usuarios por el canal de Internet Local.
	• La solución debe brindar funcionalidad de antimalware de perímetro, con integración nativa con la plataforma de Sandbox del SOC de la entidad, para la remisión de archivos sospechosos con el fin de ser analizados y detectar ataques de día cero.
	• Debe permitir la configuración de políticas de QoS en la capa 7, asociadas porcentualmente al ancho de banda de la interfaz SD-WAN
	• Debe permitir la configuración de políticas de QoS en valores donde el máximo corresponda a la totalidad del ancho de banda disponible en el equipo.
	• La solución debe integrarse de manera nativa con la plataforma de reportes de seguridad de la entidad, así como con el SIEM del SoC de la entidad.
	• Debe permitir la consulta vía SNMPv2 / v3 referente a los siguientes datos:
	  ○ Estado actual de los enlaces SD-WAN
	  ○ Latencia
	  ○ Jitter
	  ○ Packet Loss
	  ○ Paquetes enviados / paquetes recibidos
	  ○ Link Bandwitdh
	  ○ VRF asociado
	• Debe posibilitar la distribución de peso en cada uno de los enlaces que componen el SD-WAN, a criterio del administrador, de forma que el algoritmo de equilibrio utilizado pueda basarse en:
	  ○ Número de sesiones,
	  ○ Volumen de tráfico,
	  ○ IP de origen y destino
	  ○ desbordamiento de Enlace (Spillover)
	• Debe contar con la capacidad de balanceo de tráfico por paquete.
	• Debe ser capaz de admitir una arquitectura de transporte multidifusión IPv4 e IPv6 a través de túneles VPN IPSEC construidos en ADVPN.
	• Debe contar con soporte de IPv6 en overlay y underlay de SD-WAN.
	• Debe tener la capacidad de autenticar a los usuarios para la administración del equipo a través de la base de datos:
	  ○ Local
	  ○ Integrada en el servidor TACACS +
	  ○ Integrada en el servidor LDAP
	  ○ Alternativamente debe soportar base de datos centralizada propia, donde toda la arquitectura SD-WAN converge a ella

	• La Alta Disponibilidad proporcionada por La funcionalidad de SD-WAN, deberá cumplir los siguientes criterios:
	  ○ Soporte Balanceo Activo - Activo
	  ○ Soporte Balanceo Activo - Pasivo
	  ○ Soporte Balanceo de hasta 4 peers
	  ○ Soporte Balanceo Distribuido Geográficamente
	• La funcionalidad SD-WAN debe ofrecer solución de problemas en la consola de línea de comandos o gráfica, donde sea posible:
	  ○ Ejecutar Packet sniffer del tráfico interesante, filtrando por: IP y Puerto
	  ○ Realizar depuración detallada de las fases de negociación VPN
	• La funcionalidad SD-WAN debe ofrecer una visualización gráfica de:
	  ○ Aplicaciones más utilizadas con su ancho de banda
	  ○ Shaping de tráfico SD-WAN
	  ○ IP de destino más utilizados con su número de sesiones y ancho de banda asociados
	• La funcionalidad SD-WAN debe admitir la marcación de paquetes DSCP en las definiciones y reglas para el tráfico SD-WAN.

LATENCIA	La latencia es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes de datos dentro de la red (incluye el tramo satelital y el terrestre). La medición de latencias para enlaces entre puntos o de internet satelital será entre puntos conectados. El tramo satelital es donde miden la latencia definida en esta característica. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en la ficha técnica. La medición de la latencia en el tramo satelital se hará en vacío entendiendo que es posible que haya dos tramos para medir, el tramo satelital y el tramo terrestre. y que la suma de ambos debe cumplir con el valor establecido. Latencia: **< 700ms**
DISPONIBILIDAD EXIGIDA	La disponibilidad se mide usando la siguiente ecuación: $\left(1 - \frac{Número\ total\ de\ minutos\ en\ que\ el\ servico\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ contratados\ x\ 24\ horas\ x\ 60\ minutos}\right) x\ 100\%$ La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio de intercambio de datos sobre el enlace no está disponible, dividido en el número total de minutos en el mes facturado. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. Cada sede con SDWAN deberá incluir un enlace MPLS y un enlace de Internet, cada uno de estos enlaces no pueden compartir la misma última milla, ni mismo nodo del proveedor.

	La medición se hace teniendo en cuenta el conjunto de enlaces que se tendrían en la sede, es decir, la medición es por sede, en donde **cada sede debe cumplir con el valor exigido en el ANS**. **Disponibilidad exigida** **>= 99.6% mensual** **Penalidad por no conformidad - Descuento en facturación** • 98% <= disponibilidad < 99.6%: 10% de descuento sobre el costo este servicio. • 97% <= disponibilidad < 98%: 20% de descuento sobre el costo este servicio. • 95% <= disponibilidad < 97%: 50% de descuento sobre el costo este servicio. • disponibilidad < 95%: 100% de descuento sobre el costo este servicio
RTO	El RTO por sus siglas en inglés es Recovery Time Objective o en español Tiempo Objetivo de Recuperación. El RTO es el tiempo máximo que el enlace puede estar fuera de servicio una vez se ha producido una Interrupción. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. En los casos en que la interrupción sea en la herramienta de monitoreo y no en el servicio; no se contabilizará la interrupción como parte del tiempo máximo que el servicio puede estar fuera de servicio. **RTO <= 8 minutos** **Penalidad por no conformidad - Descuento en facturación** • 8 min<RTO<=15 min: 10% de descuento sobre el costo total de este servicio. • 15 min<RTO<=25 min: 20% de descuento sobre el costo total de este servicio. • 25 min<RTO<=45 min: 50% de descuento sobre el costo total de este servicio. • 45 min<RTO: 100% de descuento sobre el costo total de este servicio.
INTERRUPCIONES MÁXIMAS	El ANS Interrupciones máximas hace referencia a el número máximo de Interrupciones durante el mes facturado. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace.

	La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma por sede teniendo en cuenta el conjunto de enlaces allí instalados, es decir, cada sede debe cumplir con el valor exigido en el ANS. **Interrupciones máximas en un mes: 1 interrupción** **Penalidad por no conformidad - Descuento en facturación** • 2 interrupciones: 20% de descuento sobre el costo de este servicio. • 3 interrupciones: 50% de descuento sobre el costo de este servicio. • >4 Interrupciones: 100% de descuento sobre el costo de este servicio.
MTBF	El MTBF por sus siglas en inglés es Mean Time Between Failures o en español Tiempo Medio Entre Fallas. El MTBF es un indicador de confiabilidad definido como el promedio aritmético acumulado del tiempo entre Fallas asumiendo que el enlace se recupera de forma inmediata cuando se produce la Falla. Nota aclaratoria: El supuesto: “asumiendo que el servicio se recupera de forma inmediata” hace referencia a la forma en que se medirá en tiempo entre fallas y no a que necesariamente haya una recuperación instantánea de una falla. Una Falla se define como una degradación del servicio de conectividad con respecto a las condiciones pactadas en al Acuerdo Marco de Precios La medición la hace el Proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Proveedor para que puedan ser consultados por la el Dane en cualquier momento durante la duración del servicio. La información mantenida por el Proveedor le debe permitir a la Entidad verificar el MTBF acumulado en cualquier momento durante la prestación del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. Nota aclaratoria: Una Falla es diferente a una Interrupción. La Falla está asociada a la confiabilidad del servicio y la Interrupción está asociada a la disponibilidad del servicio. **MTBF =720 horas** • 650 horas < MTBF = 720 horas: 10% de descuento sobre el costo total de este servicio. • 500 horas < MTBF <= 650 horas: 20% de descuento sobre el costo total de este servicio. • 400 horas < MTBF <= 500 horas: 50% de descuento sobre el costo total de este servicio. • MTBF < 400 horas: 100% de descuento sobre el costo total de este servicio.

ANCHO DE BANDA	El ancho de banda corresponde al rango de frecuencias que ocupan los datos transmitidos por el enlace sin que se presente distorsión o pérdida de información. La medición la debe hacer el Proveedor una vez lo solicite el DANE por el tiempo y con la frecuencia que la Entidad lo requiera. Los resultados de la medición deben ser mantenidos por el Proveedor para que puedan ser consultadas por la Entidad durante la duración del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Ancho de banda: Debe ser igual o superior al ancho de banda contratado** **Penalidad por no conformidad - Descuento en facturación** • Si se evidencia una reducción del 10% sobre el ancho de banda contratado: 40% de descuento sobre el costo del servicio • Si se evidencia una reducción del 20% sobre el ancho de banda contratado: 50% de descuento sobre el costo del servicio • Si se evidencia una reducción >= 30% sobre el ancho de banda contratado: 100% de descuento sobre el costo del servicio
CALIDAD Y OPORTUNIDAD EN LOS REPORTES ENTREGADOS	El Proveedor debe garantizar la calidad de la información que contienen los reportes que entrega a la Entidad. Con el fin de garantizar la calidad de los reportes se define el número máximo de devoluciones en que puede incurrir el Proveedor sin que se generen penalizaciones para cada nivel de servicio. Adicionalmente, se establecen las penalidades por no conformidad que se le harán al Proveedor cuando supera el número máximo de devoluciones. **Devoluciones máximas por cada reporte:** **<= 2 devoluciones de un mismo reporte** **Penalidad por no conformidad - Descuento en facturación** • 3 devoluciones del mismo reporte: 10% • 4 devoluciones del mismo reporte: 20% • 5 devoluciones del mismo reporte: 50% • 6 devoluciones del mismo reporte: 100%
ELASTICIDAD	**Crecimiento definitivo** Ampliaciones definitivas en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. Una ampliación definitiva tiene una duración correspondiente al tiempo restante de servicio. Capacidad de crecimiento: Hasta el 100% sin cambio de equipos. **Crecimiento temporal** Ampliaciones en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. • Capacidad de crecimiento: Hasta el 100% sin cambio de equipos

	Duración del crecimiento • Mínima (días): Entre 7 días calendario hasta 30 días calendario Máxima (mensual): 60 días calendario
TIEMPO DE APROVISIONAMIENTO DE CRECIMIENTOS CONTEMPLADOS EN EL NIVEL DE ELASTICIDAD CONTRATADO	El crecimiento de los enlaces está dado por las características de elasticidad definidas en esta ficha. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Elasticidad alta** **<= a 16 horas continuas** **Penalidad por no conformidad - Descuento en facturación** • 2 horas continuas de retraso: 10% de descuento sobre el costo este servicio. • 4 horas continuas de retraso: 20% de descuento sobre el costo este servicio. • 6 horas continuas de retraso: 50% de descuento sobre el costo este servicio. • 8 horas continuas de retraso: 100% de descuento sobre el costo este servicio.
EFECTIVIDAD EN RESOLUCIÓN DE INCIDENTES/SOLICITUDES	Aplicable para: • Solicitudes de cambios • Cambios en configuraciones • Habilitación de VPN. • Resolución de inquietudes • Entrega reportes e información. • Solución de incidentes La efectividad de resolución de solicitudes mide el tiempo máximo de solución de las solicitudes realizadas a la mesa de ayuda del Proveedor según su nivel de prioridad. El reloj que mide la efectividad de resolución comienza a contabilizar el tiempo desde el momento en que el ticket es registrado en la mesa de ayuda hasta que el Proveedor da una respuesta y soluciona el problema. Zona 1: • Prioridad 1: Efectividad de resolución <=4 horas • Prioridad 2: Efectividad de resolución <= 18 horas • Prioridad 3: Efectividad de resolución <= 64 horas Zona 2: • Prioridad 1: Efectividad de resolución <= 8 horas • Prioridad 2: Efectividad de resolución <= 32 horas • Prioridad 3: Efectividad de resolución <= 88 horas Zona 3 y 4: • Prioridad 1: Efectividad de resolución <= 20 horas • Prioridad 2: Efectividad de resolución <= 48 horas Prioridad 3: Efectividad de resolución <= 112 horas Un incidente puede causar:

	Interrupción no planeada del servicio. Reducción de la calidad del mismo. Falla de un servidor que todavía no ha impactado un servicio. Prioridad 1: Son los casos por eventos cuando afecta al core del negocio, si este no se llegase a solucionar con reinicio, se maneja como IM (Incidente Mayor). Prioridad 2: Cuando no se ha afectado la disponibilidad del servicio total, pero hay un alto riesgo Prioridad 3: Afectación de un servidor no core. Un server caído de un ambiente de pruebas.
HARDWARE Y SOFTWARE	El Proveedor debe garantizar toda la conectividad física y lógica requerida para la puesta en funcionamiento de los servicios y conectividad contratada. La conectividad física hace referencia a todos los elementos de hardware necesarios para proveer el servicio. (El DANE dispone de las condiciones de infraestructura para la entrega del servicio, tales como: energía regulada, sistema de puesta a tierra, rack y espacios de comunicaciones para instalar equipos de telecomunicaciones y condiciones ambientales óptimas para la temperatura de los equipos, esto en el caso que los servicios contratados así lo requieran). La conectividad lógica hace referencia a todos los elementos de software necesarios y su respectiva configuración para proveer el servicio.
NAP COLOMBIA	El ISP (Internet Service Provider) debe incluir conexión al NAP Colombia garantizando el 100% del ancho de banda contratado por parte de la Entidad compradora, garantizando que el tráfico de datos que tiene origen y destino en el territorio nacional no transite por enlaces internacionales y en conformidad a lo establecido en la Res. CRC 5078 de 2016 "Indicadores de Calidad" Res. 5050 "compilada de las resoluciones de carácter general" y todas aquellas que adicionen, modifiquen o sustituyan.
ENLACES DE SALIDA INTERNACIONAL A INTERNET	El Proveedor debe contar con al menos dos salidas a Internet internacional (medios físicos de salida diferentes) que deben ser configuradas para permitir el direccionamiento en compatibilidad IPv4 e IPv6. El Proveedor debe ofrecer para las salidas internacionales a internet, enlaces de comunicaciones de alta disponibilidad capaces de soportar el tráfico y compatibilidad de IPv4 e IPv6 simultáneo sin inconvenientes de ancho de banda. Esta condición podrá ser cumplida ya sea de manera directa o a través del proveedor con el que tenga el convenio correspondiente.
REGISTRO TIC	El Proveedor para la prestación de los servicios de telecomunicaciones solicitados, deberá contar con el Registro TIC emitido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones el cual lo acredita como Proveedor de Redes y Servicios de Telecomunicaciones en el territorio nacional. El Registro TIC deberá estar vigente durante toda la ejecución del contrato.
AISLAMIENTO DE RED	El Proveedor debe garantizar que el servicio de conectividad admite controles de aislamiento de red para tráfico entrante y saliente a través de métodos a nivel de capa 2 o 3. El Proveedor debe articular cualquier restricción, condición o requisito de red, como la traducción de dirección de red (NAT), la superposición de direcciones IP y controles de latencia para los procesos de traducción NAT.

SERVICIO DE SOPORTE TÉCNICO	El Proveedor debe tener la capacidad de brindar servicio de soporte técnico remoto y en sitio para los servicios contratados por la Entidad. El Proveedor debe brindar soporte en sitio para evaluar y solucionar Fallas e Interrupciones que se presenten en los servicios contratados por la Entidad Compradora. El soporte será en sitio sólo en los casos en que no sea posible resolver el problema de forma remota. El servicio en sitio no significa costos adicionales para el DANE. Adicionalmente, el Proveedor debe brindar soporte remoto a nivel nacional a través de los siguientes canales: - Línea de atención telefónica gratuita con cobertura nacional. - Plataforma web para registro y monitoreo de tiquetes. - Correo electrónico. - Chat. El Proveedor debe garantizar que cuenta con un servicio de mesa de ayuda el cual deberá operar en instalaciones a cargo del proveedor. El Proveedor debe garantizar que exista un tiquete por cada reporte de Falla o Interrupción que haga el DANE. Los canales de soporte deben estar disponibles 7x24 durante el tiempo de ejecución del contrato. El grupo de soporte del Proveedor debe garantizar que los tickets: • Sean registrados, clasificados y asignados según su criticidad. • Sean resueltos en los tiempos acordados en los ANS. • Tengan un seguimiento adecuado. • Cumplan con esquemas de escalamiento definidos. Deben ser documentados con las respectivas evidencias y en caso de requerir atención en sitio anexar registros fotográficos donde se observe Georreferenciación, fecha y hora donde ocurrió el evento. El proveedor debe garantizar que cuenta con la especialidad de SD_WAN del fabricante de la solución, esta certificación debe emitirla el fabricante, estar dirigida a la entidad e indicar el número del proceso.
SERVICIO DE SOPORTE TÉCNICO - EFECTIVIDAD EN LA ATENCIÓN DE LOS CANALES	El Proveedor debe garantizar tiempos de efectividad en la atención para cada canal como se detalla a continuación: • Línea telefónica nacional gratuita: <= 5 minutos. • Plataforma web para registro y monitoreo de tiquetes: <= 2 minutos. • Correo electrónico: <= 5 minutos. • Chat: <= 3 minutos.
SERVICIO DE SOPORTE TÉCNICO - NIVELES DE ATENCIÓN Y ESCALAMIENTO	El Proveedor debe Incluir el servicio de soporte técnico para el manejo de niveles 1 y 2 de soporte. Adicionalmente, el servicio de soporte técnico suministrado por el Proveedor debe gestionar escalamientos a nivel 3 o superior cuando corresponda. El proveedor del servicio de conectividad al inicio de la ejecución del contrato deberá entregar un documento en el que indique el nivel de escalamiento (Nombre

	del profesional, cargo, correo electrónico y número de celular de contacto) con al menos tres (3) profesionales asignados por el proveedor que permitan, elevar los requerimientos en caso de la no atención satisfactoria de las solicitudes. los perfiles asignados deberán ser al menos en el nivel 1. tecnólogo, y en los niveles 2 y 3 profesionales con vinculación con el proponente.
SERVICIO DE SOPORTE TÉCNICO - PRIORIZACIÓN DE TICKETS	Los tiquetes deben ser clasificados y atendidos según su nivel de criticidad. Los criterios para llevar a cabo dicha clasificación son los siguientes: **Prioridad 1:** Emergencia - Una Falla que afecta un proceso critico de la Entidad. **Prioridad 2:** Degradación en el servicio - Una Falla que afecta el desempeño o confiabilidad de un proceso de la Entidad. **Prioridad 3:** Inquietud o solicitud - Solicitudes de soporte menores o de información que no tienen impacto en los procesos de la Entidad. Incluye: Solicitudes de cambios, cambios en configuraciones, habilitación de VPN, resolución de inquietudes y entrega de información.
SERVICIO DE SOPORTE TÉCNICO - REPORTES DE GESTIÓN	El Proveedor debe entregar reportes mensuales de mesa de ayuda al supervisor del contrato, que permitan monitorear las siguientes variables: • Número de incidentes reportados según nivel de criticidad. • Número de incidentes resueltos que incluya el tiempo promedio de resolución según nivel de criticidad. • Análisis de causa raíz para incidentes relacionados. • Propuestas de mejora continua para los servicios contratados. • 2 variables más que defina la Entidad Compradora. La Entidad Compradora definirá las variables teniendo en cuenta que puedan ser soportados por la herramienta de monitoreo del Proveedor. El Proveedor debe entregar un reporte consolidado de mesa de ayuda una vez concluya el servicio de conectividad contratado. El proveedor debe contar con una plataforma que le permita al DANE visualizar consumo de canales en tiempo real y enviar reportes automáticos mensuales.
OBRA CIVIL	El servicio suministrado por el Proveedor incluye los costos y responsabilidades que significa adecuar la obra civil en cada uno de los puntos indicados donde se requiere el servicio. En caso de que se requiera y de ser necesario adelantar una obra civil, en las instalaciones de la Entidad o alguna de sus sedes, esta se entiende como: canalización con tubería EMT (Electrical Metallic Tubing), que corresponde al tendido de cables instalados a través de canalizaciones que contienen los ductos que permiten el tendido, la protección y el mantenimiento de cables de red y también de cables de fibra óptica. Se debe contemplar la instalación, adecuación y señalización de cables o fibra sobre canaletas de las instalaciones de la Entidad. El Proveedor debe estimar el costo total de la obra civil desde la acometida hasta el punto donde la Entidad requiere el enlace e incluirlo en el valor de instalación.

	Los costos en que incurra el Proveedor por la obra civil desde sus instalaciones (las del Proveedor) hasta la acometida en las sedes de la Entidad son responsabilidad del Proveedor.
TIEMPOS DE INSTALACIÓN	Es el tiempo máximo que puede tardar el Proveedor en hacer las instalaciones sin incurrir en incumplimiento, los cuales se solicitan de la siguiente manera: <= **35 días calendario** El proveedor entrante debe garantizar una transición controlada con el proveedor actual, evitando que se presenten interrupciones en ninguno de los servicios que actualmente brinda la Entidad a los usuarios. En este sentido, el proveedor entrante deberá asumir todos los costos asociados con la continuidad actual del servicio durante el tiempo necesario para llevar a cabo sus propias instalaciones y configuraciones, de manera que la Entidad no experimente ninguna indisponibilidad del servicio, hasta que esté plenamente instalada la solución del nuevo operador a satisfacción de la Entidad.
ANÁLISIS DE VULNERABILIDADES	El proveedor deberá ejecutar de forma semestral un análisis de vulnerabilidades sobre la infraestructura utilizada para la prestación de los servicios de conectividad, incluyendo herramientas de gestión, plataformas de seguridad, equipos de borde, canales de acceso a internet y dispositivos de red entre otros. El análisis de vulnerabilidades deberá ejecutarse usando una herramienta licenciada, no open source, en esquema empresarial, que cuente con todas las actualizaciones que el fabricante de la herramienta disponga en términos de vulnerabilidades reportadas. Adicionalmente el Proveedor presentará el informe de las vulnerabilidades identificadas en las pruebas, según requerimiento de la entidad compradora, dentro de los siguientes 3 días hábiles posteriores a la solicitud. La prueba debe incluir como mínimo las IP, sistemas operativos y las vulnerabilidades detectadas de los sistemas escaneados. Este reporte deberá ser entregado al supervisor del contrato según su solicitud, incluyendo los requisitos establecidos**.**
NOTIFICACIÓN DE INCIDENTES Y ENTREGA DE INFORMES DE INDISPONIBILIDAD	El proveedor del servicio deberá notificar los incidentes mediante al menos dos medios diferentes de comunicaciones (SMS, Correo electrónico, aplicaciones como WhatsApp, entre otros) que la Entidad determine y al personal que defina. Adicionalmente la Entidad, podrá establecer o delimitar el tipo de incidentes desea que le sean reportados de acuerdo con el nivel de criticidad. El proveedor del servicio tendrá 24 horas a partir del momento de un incidente crítico para reportarle a la Entidad Compradora el informe detallado. En el cual deberá relacionar al menos motivo de la falla, tiempo de indisponibilidad, elementos y servicios afectados, mecanismo utilizado en la solución del incidente crítico y mecanismos de prevención del incidente a futuro. El proveedor del servicio determinará el formato utilizado para el informe siempre y cuando se cuente con al menos la información solicitada.
RESPONSABILIDADES	El Proveedor administra la seguridad de la infraestructura y servicios de los elementos que tiene bajo su responsabilidad para la prestación de servicio. El Proveedor pondrá a disposición la tecnología necesaria para garantizar la seguridad de los servicios: autenticación, cifrado y controles de conexión a la red.

	Adicionalmente, el Proveedor suministrará los parámetros técnicos y procedimientos para garantizar la seguridad de los servicios.
QoS y CoS	El Proveedor debe brindar en los enlaces QoS (Calidad de Servicio) y CoS (Clase de Servicio) en los casos en que la Entidad Compradora lo requiera.
PROTOCOLO SNMP	El Proveedor debe garantizar que todos los equipos necesarios, tienen habilitado el protocolo SNMP para poder supervisar el funcionamiento de la red.
PLATAFORMA DE MONITOREO	El Proveedor debe proporcionar una plataforma de monitoreo y uso de tráfico en vivo en la cual se pueda consultar el estado de los canales y el uso de estos mediante un servicio web para lo cual el proveedor deberá entregar al menos 2 usuarios para el uso de la Entidad. La plataforma debe mantener los resultados del monitoreo con gráficas, históricos de meses anteriores y para el mes en curso en tiempo real (con un retraso menor a 5 minutos), para que puedan ser consultados por la Entidad Compradora en cualquier momento durante la duración del servicio. La retención de la información corresponderá a toda la vigencia del contrato y podrá ser entregada a la entidad, previa solicitud, una vez finalizado el servicio. Los indicadores a monitorear incluyen las variables asociadas a los ANS que especifica cada ficha de servicio.
REPORTE DE GESTIÓN	El Proveedor debe monitorear y entregar un reporte de gestión a la Entidad incluido los eventos, la capacidad, la seguridad y la utilización de los diferentes componentes de los servicios de conectividad suministrados. El reporte de gestión debe incluir los resultados del seguimiento hecho durante el mes de los indicadores que a continuación se listan: - Disponibilidad. - Número máximo de interrupciones. - RTO. - MTBF. - Latencia. - Ancho de banda. Adicionalmente, para los servicios de enlaces terrestres y satelitales el Proveedor debe monitorear las siguientes variables: - Tráfico de entrada. - Tráfico de salida. El reporte de gestión del servicio que entrega el Proveedor debe contener, además; información de uso de los componentes de infraestructura que componen el servicio (ejemplo: ancho de banda consumida en línea de tiempo durante el periodo, VPNs configuradas, tráfico en el administrador del ancho de banda y eventos reportados por el firewall). El criterio de evaluación de calidad de los reportes hace referencia a que incluya todo el contenido detallado anteriormente." El Proveedor debe entregar los reportes de gestión y calidad del servicio y de cada componente que lo constituye con una periodicidad igual a la frecuencia de facturación.
DESCUENTOS EN FACTURACIÓN	El valor máximo de los descuentos corresponde al 100% del valor del servicio facturado aun cuando la suma total de los descuentos supere 100%.

DAÑOS Y MAL FUNCIONAMIENTO DE EQUIPOS	El Proveedor 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.
MANTENIMIENTO	El Contratista es responsable del mantenimiento de los equipos y dispositivos entregados por su cuenta para el desarrollo del contrato, de esta forma es su responsabilidad realizar mantenimientos preventivos y correctivos con el fin de garantizar el cumplimiento de los acuerdos de nivel de servicio (ANS).

1.3 SEGURIDAD INFORMÁTICA

GENERALIDADES	La Entidad requiere contar con el servicio de aseguramiento de la plataforma tecnológica, la cual está enfocada en proteger los servicios críticos de la entidad, los cuales deben operar de manera ininterrumpida, contemplando la trazabilidad sobre la información y eventos de seguridad, tomando las medidas pertinentes con respecto a riesgos informáticos. Los servicios de seguridad informática son requeridos para instalarse en la sede principal del DANE Carrera 59 # 26 - 70 CAN Interior 1 en la ciudad de Bogotá. El proveedor debe realizar la implementación, configuración y puesta en marcha de todas las soluciones que hacen parte del servicio. Se requiere alinear el servicio con las políticas de seguridad de la información de la entidad, realizando las configuraciones necesarias en cada plataforma para garantizar la prestación del servicio. El proveedor deberá configurar el servicio teniendo en cuenta las mejores prácticas de seguridad, para esto la entidad realizará una revisión de las configuraciones de las plataformas, a fin de constatar que la totalidad de los módulos de las soluciones que aprovisionan el servicio se encuentre configurados y licenciados. El oferente deberá contar con un SOC para la gestión de incidentes de seguridad que se encuentre ubicado dentro del territorio nacional y sea miembro de FIRST (Fórum of Incident Response and Security Teams) con una madurez en la membresía de mínimo 9 años. Para lo anterior, el Oferente deberá adjuntar evidencia directa de la página web oficial de la suscripción al FIRST, en donde se identifique que el país del equipo sea Colombia (Country of Team Colombia) y carta de representante legal que acredite el cumplimiento de esta condición. **NOTA**: **El proveedor deberá ofrecer toda la asistencia técnica necesaria para respaldar las plataformas y, en caso de ser necesario, asumir la administración de estas cuando así lo requiera el DANE.** Las soluciones que requiere la Entidad se detallan a continuación:
APPLIANCE FIREWALL DE NUEVA GENERACIÓN NGFW	Solución de propósito específico mediante un appliance Firewall de nueva generación que debe estar en configurada en alta disponibilidad a instalar en la sede principal del DANE Carrera 59 # 26 - 70 CAN Interior 1, Bogotá. Los equipos de seguridad Firewall de nueva generación (NGFW), empleados para la prestación de los servicios objeto del presente proceso, deben ser nuevos con tiempo de fabricación no superior a un (1) año certificado por el respectivo fabricante, por consiguiente, no se aceptarán equipos remanufacturados ni repotenciados.

	Se requiere al proveedor que desde el inicio de la ejecución contractual los equipos Firewall queden como propiedad de la Entidad con garantía y licenciamiento de tres (3) años, es decir se adquieren por parte del DANE. Se debe garantizar por parte del proveedor que la solución de seguridad perimetral tenga una disponibilidad de 99.9% 7x24 durante la duración del contrato. Se debe garantizar por parte del proveedor que los servicios de firewall de nueva generación se encuentren como líderes en el Cuadrante Mágico de Gartner. A continuación, se relacionan las características mínimas de obligatorio cumplimiento, los cuales deberán ser demostrables por medio de las fichas de datos públicas del fabricante, por lo cual no se aceptan cartas de fabricante del tipo Ad-Hoc para soportar estas: • Rendimiento de FW mínimo 220 Gbps. • Rendimiento de IPS: mínimo 34 Gbps. • Rendimiento VPN IPSEC: mínimo 95 Gbps. • Rendimiento Inspección SSL: mínimo 10 Gbps. • Soporte mínimo 65.000.000 sesiones concurrentes. • Soporte mínimo 800.000 de nuevas sesiones por segundo. • Soporte mínimo 30.000 usuarios VPN SSL, sin requerir de licenciamiento. • La plataforma deberá integrarse de forma nativa sin requerir desarrollos a adicionales a la solución de Gestión y Reportes con la que cuenta la entidad. • Soporte de al menos 30 Gbps de desempeño de Protección de Amenazas, medido con tráfico empresarial. • Tener al menos 6 puertos de 100 / 40 GE • Tener al menos 16 puertos de 25 GE SFP28 / 10 GE SFP+ • Tener al menos 16 puertos 10 GE / GE RJ45 • Tener al menos 2 puertos de 25 GE SFP28 / 10 GE SFP+ / SFP para alta disponibilidad • Tener al menos 1 TB de almacenamiento interno • Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance • Se debe poder ver el consumo de CPU y memoria de cada instancia virtual. • La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. • Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual. • Dos (2) equipos en Clúster en capacidad de funcionar en un esquema Activo-Activo o Activo-Pasivo, según requiera la entidad. Requisitos Mínimos de Funcionalidad: A continuación, se relacionan los requisitos mínimos funcionales de obligatorio cumplimiento, los cuales deberán ser demostrables por medio de documentación pública del fabricante, por lo cual no se aceptan cartas de fabricante del tipo Ad-Hoc para soportar las mismas: • La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW). • Por funcionalidades de NGFW se entiende: Firewall, control de aplicaciones, prevención de amenazas, Filtrado de Contenido, Filtrado de DNS, DoS, identificación de usuarios, VPN IPSec, VPN SSL y prevención de fuga de información.

	• La solución debe brindar las funcionalidades de: Firewall, IPS, Control de Aplicaciones, Filtrado Web, Antivirus perimetral, SD-WAN, Sandboxing y DLP. • La solución debe permitir la definición de reglas y objetos para IPv4 e IPv6 via GUI y CLI • La solución debe soportar implementación de SD-WAN, para manejo de conectividad hacia las sedes remotas de la entidad y hacia el datacenter onpremises. • La solución debe tener soporte de NAT estático, NAT dinámico, PAT, NAT64, NAT46, NAT66. • La solución debe tener soporte a reglas basadas en servicios cloud populares de Internet (al menos Adobe Cloud, Alibaba Cloud, Amazon AWS, Atlassian Cloud, Bitdefender, Bloomberg. Cisco Duo, Cloudflare, Azure, Google Cloud y Facebook), en donde se tiene una base de datos que se actualiza dinámicamente. Esta base de datos puede usarse también en enrutamiento y balanceo de enlaces o SD-WAN. • La solución debe tener soporte de OSPFv2, IS-IS y BGP para IPv4, y soporte de RIPng, OSPFv3, IS-IS y BGP para IPv6. • Soporte incluido y listo para ser configurado de SD-WAN tanto para IPv4 como para IPv6, en underlay y overlay. para la distribución de tráfico entre varios enlaces WAN. • La solución debe permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en categorías del fabricante, para IPv4 e IPv6. • La solución de Filtrado de Contenido debe soportar la característica de “Safe Search” o “Búsqueda Segura” para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes sitios: Google, Yahoo, Bing y Yandex. • El filtrado de contenido web debe permitir la definición de palabras, frases, patrones, wildcards y expresiones regulares Perl para prevenir acceso a páginas con material cuestionable. • El filtrado web debe poder bloquear tráfico a sitios de acortado de URLs (URL shortening). • La solución debe estar en capacidad de hacer inspección de tráfico DNS, incluyendo tráfico DoT (DNS over TLS) y DoH (DNS over HTTPS). • El módulo de IPS debe mitigar los efectos de los ataques de negación de servicios. • Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP, HTTPS, IMAPS, POP3S, SMTPS y FTPS y CIFS tanto para IPv4 como IPv6. • La solución debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS. • Debe soportar integración con la plataforma de Sandbox del SOC de la entidad, para la remisión de archivos sospechosos con el fin de ser analizados y detectar ataques de día cero. • La solución debe poder hacer inspección de tráfico cifrado para TLS v1.3 • Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad. • La solución debe tener capacidad de definición de sensores de información sensible basados en tipo de archivo, tamaño de archivo, expresión regular y combinación de estos criterios.

	• La solución debe contar con interface gráfica de usuario (GUI), vía Web por HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente, sin requerir de instalación de software adicional. Debe contar también con Interfase basada en línea de comando (CLI) para administración de la solución. • La solución debe permitir el acceso para administración de dispositivos remotos del mismo fabricante desde la GUI del firewall una vez estos se encuentren integrados, sin requerir consola o licenciamiento adicional. • La solución debe permitir la visualización de la topología física y lógica, con el fin de obtener más información de los dispositivos y conexiones, como por ejemplo visualizar el web application firewall en la topología. • La solución debe permitir exportar el listado de políticas en formato CSV y JSON. • La solución debe permitir hacer rollback de los cambios de configuración realizados si no se confirman durante un lapso de tiempo configurable. • La solución NGFW debe soportar gestión de identidad y acceso mediante una solución de autenticación multifactor MFA. • La solución debe soportar integración con NGFW y LDAP o Active Directory para aplicar políticas de grupo o rol al usuario. • La solución debe proveer un servicio de autenticación en la cual los usuarios reciban un token gestión de identidad y acceso mediante una solución de autenticación multifactor MFA. • El proveedor deberá suministrar 4.000 tokens de software, para el acceso VPN compatibles con la marca de firewall de nueva generación que deben estar licenciados a perpetuidad. • El proveedor deberá suministrar todos los elementos (fibras, cables, transceivers, etc, necesarios para hacer funcional la solución). • El proveedor deberá realizar el monitoreo de los equipos de seguridad perimetral a través de su SOC realizando la correlación de eventos.
APPLIANCE FIREWALL DE APLICACIONES WAF	Servicio mediante una solución de propósito específico del tipo appliance dedicado a la protección de aplicaciones WEB del tipo Web Application Firewall que se debe instalar en la sede principal del DANE Carrera 59 # 26 - 70 CAN Interior 1, Bogotá. Los equipos de seguridad Web Application Firewall (WAF), empleados para la prestación de los servicios objeto del presente proceso, debe encontrarse en su periodo de vida útil durante y debidamente licenciado durante el periodo de ejecución del contrato e implementado en la versión más estable del fabricante. Se solicita que esta solución se entregue con un (1) solo equipo no se solicita alta disponibilidad para este servicio. La solución debe cumplir con las siguientes características mínimas: • La solución deberá contar con soporte de fabricante durante el tiempo de contrato. • La solución debe de soportar enrutamiento por política (policy route) • Debe configurarse eficientemente para proteger las Aplicaciones Web de la entidad de amenazas externas, con el rendimiento necesario para proteger otros portales web que la entidad publique sin requerir licenciamiento adicional. • La solución debe poder restaurar los portales web de forma automática en caso de presentarse una modificación no autorizada. La solución contar con un módulo de anti-defacement el cual permita monitorear las aplicaciones, alertar y de ser necesario restaurar en caso de modificaciones no autorizadas de las aplicaciones web protegidas, la

	solución debe poder monitorear la integridad de los archivos por medio de FTP, SSH o SMB, por lo tanto, no se acepta soluciones que requieran la instalación de agentes, los cuales agreguen más carga a los servidores. • La plataforma propuesta debe identificar vulnerabilidades a un número ilimitado de aplicativos web de la entidad, sin requerir licenciamiento adicional. • En caso de ser requerido la solución debe realizar balanceo de tráfico para garantizar disponibilidad de las aplicaciones web protegidas. • La solución deberá contar con sus respectivas actualizaciones periódicas a nivel de firmas de seguridad durante el periodo contratado. • La solución deberá ser totalmente compatible con IPv6. • La solución debe poderse implementar en modo proxy reverso, transparente o monitoreo. Sin embargo, en conjunto con la entidad se definirá la mejor opción a nivel de configuración de seguridad. • La solución debe integrarse con la plataforma de logs y reportería de seguridad de la entidad de manera nativa. • La solución deberá integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo de la garantía. Con esto la herramienta debe ser capaz de proteger de las siguientes amenazas: • Cross-Site Scripting (XSS) • SQL Injection • Remote File Inclusion • Local File Inclusion • OS Commands • Troyanos y virus • Exploits • Información Sensible del servidor • Firmas personalizadas • Adobe Flash Binary (AMF) protocol Attack. • Botnet • Browser Exploit Against SSL /TLS • Clickjacking • Cookie Tampering • Credit Card Theft • Cross Site request forgery • HTTP Header Overflow • Malicious Robots • Man in the Middle • Server information leakage • Malformed XML • La solución deberá contar con un módulo de prevención contra ataques de denegación de servicio en http y https de tal forma que proteja a las aplicaciones web contra este tipo de ataques, dicho módulo deberá permitir como mínimo las siguientes acciones: • Alertar. • Denegar. • Bloquear por un Periodo de Tiempo. • La solución debe contar con protección basada en Machine Learning (ML) con dos etapas independientes, para la detección de anomalías en los parámetros de las aplicaciones web, identificación de ataques y para protección contra bots. • La solución deberá contar con un módulo de escaneo AntiMalware para hacer una revisión de los archivos que sean posteados o subidos a las aplicaciones web, permitiendo ejecutar las siguientes acciones: • Detección y bloqueo de malware conocido a nivel de los archivos que se suben a las aplicaciones web.

	• Debe soportar integración con la plataforma de Sandbox del SOC de la entidad, para la remisión de archivos sospechosos con el fin de ser analizados y detectar ataques de día cero. • Integración nativa con la plataforma de SIEM del SOC de la entidad. • Integración nativa con el Firewall de Nueva Generación ofertada, para el intercambio de IP de cuarentena. • La solución deberá contar con un módulo para la prevención de fuga de información, la cual permite crear reglas personalizadas basadas en patrones, este módulo deberá ser completamente funcional sin requerir licencias adicionales o integraciones con plataformas de terceros. • El proveedor deberá suministrar todos los elementos (fibras, cables, transceivers, etc, necesarios para hacer funcional la solución) Características mínimas de la solución WAF: • Throughput HTTP mínimo de 20 Gbps • Número de aplicaciones web a proteger y que deben entregarse aseguradas con el WAF: Ilimitado. • 8 interfaces de red GE RJ45. • 4 interfaces de 1 Gbps SFP • 4 interfaces de 10 Gbps Funcionalidades de Web Application Firewall: • Debe tener soporte nativo de HTTP/2 • Debe soportar traducción de HTTP/2 a HTTP 1.1 • Deberá soportar interoperabilidad con OpenAPI 3.0 • Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica • La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus. • Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no • Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial • Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo • El perfil aprendido de forma automática debe de poder ser ajustado • Tener la capacidad de creación de firmas personalizadas de ataques • Tener la capacidad de protección contra ataques del tipo Botnet • Debe soportar detección de ataques de Clickjacking • Debe soportar detección de ataques de alteración de cookie • Tener la capacidad de protección contra ataques del tipo HTTP header overflow • Identificar y prevenir ataques del tipo Low-rate DoS • Prevención contra Slow POST attack • Proteger contra ataques Slowloris
APPLIANCE MODULADOR DE TRÁFICO	Servicio de administración de ancho de banda licenciado para una capacidad mínima de 2.5Gbps. El equipo debe soportar realizar crecimientos a través de licenciamiento adicional hasta una capacidad de 8Gbps.

	Proveer el servicio de gestión de tráfico físico en la sede principal del DANE Carrera 59 No. 26-70 Interior I - CAN, a través de un equipo de propósito específico, que debe soportar: • El equipo debe estar licenciado para soportar una capacidad mínima de 2.5Gbps. • El equipo debe tener la posibilidad de escalar hasta 8 Gbps, adquiriendo licenciamiento por demanda (sin compra de hardware adicional). • El equipo deberá contar con módulo de bypass externo y pasivo, que permita realizar el remplazo del equipo sin interrumpir la continuidad de la conectividad de los enlaces. • Soporte a identificación y tratamiento de tráfico sobre IPv6 e IPv4. • La solución deberá contar con soporte de fabricante durante el tiempo de contrato. • El proveedor deberá suministrar todos los elementos (fibras, cables, transceivers, etc, necesarios para hacer funcional la solución). La solución debe cumplir con las siguientes características mínimas: • La solución de Administración de Ancho de Banda debe integrarse a la red de forma transparente en capa 2 y debe permitir priorizar la asignación de ancho de banda a las aplicaciones y servicios misionales del DANE. • La solución de Administración de Ancho de Banda debe dar cobertura a un canal de internet compuesto por dos (2) segmentos físicos en Fibra Óptica de 10GE SR. • La solución debe incluir interfaces de gestión (Management Ports) independientes de los puertos de producción. • La solución de Administración de Ancho de Banda debe soportar IPv4 e IPv6. • La solución de Administración de Ancho de Banda debe incluir doble fuente de poder • La solución de Administración de Ancho de Banda debe estar licenciada para 2.5 Gbps • La solución de Administración de Ancho de Banda debe estar licenciada para soportar una capacidad mínima de 4,5 millones de "IP Flows". Funcionalidades: • Se requiere que la tecnología ofertada este dedicada a la funcionalidad de Administración de Ancho de Banda, no se aceptan soluciones con “funcionalidades secundarias” de QoS como UTM, NGFW, enrutadores o soluciones similares las cuales son limitadas y no cumplen con el requerimiento de la entidad. • El equipo ofertado debe contar con una consola de gestión y reportes. • El equipo debe permitir el envío de alarmas de uso de ancho de banda o de eventos en el sistema vía SNMP. • La solución de Administración de Ancho de Banda debe tener al menos tres (3) niveles de clasificación (jerarquías) en la creación de las políticas y soportar al menos 50.000 políticas. • Capacidad de varios niveles de Qos, en función del tipo de tráfico usando los estándares Drop Precedence, Assured forwarding, Expedited Forwarding. • Clasificación de tráfico por VLAN, por dirección IP, red(subred)/rango de IP, aplicación, TOS y horarios donde todos estos criterios se puedan usar al tiempo en una o varias políticas. • Capacidad de clasificar y asignar QoS al tráfico en función de la hora del día

	• El equipo debe contar con categorías de navegación (similares a las de un proxy) que permitan asignar políticas de ancho de banda a categorías de navegación como juegos, páginas gubernamentales etc.
	• Capacidad de clasificar tráfico en VLAN (soporte del protocolo 802.1q).
	• Soporte avanzado de aplicaciones P2P. Por ejemplo, se reconocer aplicaciones P2P encriptadas en SSL.
	• El sistema ofertado debe soportar el reconocimiento de al menos los siguientes protocolos: Deezer, Spotify, Claro Video, Netflix, Instagram, Whatsapp (voz, Video). Microsoft Teams, Office 365 (Outlook, one drive, SharePoint) Google Maps, Google Music, drive, Apple Siri, Apple FaceTime (voice and video), Icloud, Itunes, TikTok, Waze, Lock4Shell.
	• El equipo debe contener firmas que le permitan identificar anonimizers tipo VPN o tipo TOR y tráfico de criptomonedas sin necesidad de módulos adicionales.
	• Gestión de ancho de banda independiente en cada sentido de la comunicación (subida y bajada)
	• Posibilidad de definir Templates de reglas de QoS (tipo planes de servicio) para poder generar un gran número de reglas iguales de una forma fácil y escalable.
	• El sistema debe ser actualizado en su catálogo de firmas de identificación de tráfico por el fabricante al menos dos veces por mes
	• Las versiones de firmas de protocolos deben ser modificables en su versión y en los protocolos incluidos de tal manera que se pueda decidir la versión a instalar y si se desea o no actualizar o agregar algún protocolo.
	• Las actualizaciones de los protocolos se deben realizar sin necesidad de reinicio o cambio de firmware de los equipos
	• Posibilidad de que el cliente defina sus propias aplicaciones y que pueda gestionar el ancho de banda asociado a ellas.
	• Definición de Alertas que permitan superados determinados umbrales de consumo de tráfico de una política, generar una alarma y/o enviar un correo electrónico.
	• Herramienta de gestión centralizada:
	  ○ Monitoriza hasta 2 horas de información en tiempo real
	  ○ Reportes históricos, hasta un (1) año de información en tiempo pasado.
	  ○ Reportes en tiempo real, resolución de 30 segundos
	  ○ Capacidad de generar informes de consumo por aplicación
	  ○ Capacidad de generar informes de las conversaciones entre múltiples IP's
	  ○ Capacidad de programar la generación de informes. Estos informes se podrán enviar en diferentes formatos como: pdf, html, jpg o csv
	  ○ La plataforma ofertada debe poder ser monitoreada vía SNMP
	  ○ El acceso a la gestión debe permitir el manejo de al menos 3 perfiles (Administrador, operador y Monitoreo)
	• El oferente debe presentar carta emitida por el fabricante de la solución ofertada en donde confirme que es partner autorizado para el suministro, instalación y soporte de los equipos que hacen parte de la solución y el cumplimiento del 100% de los requerimientos técnicos detallados en el presente documento.
	• Los servicios profesiones de implementación deben ser avalados presentando carta del fabricante de la solución ofertada.

APPLIANCE ANTIDDoS	Servicio mediante un Appliance AntiDDoS licenciado para una capacidad de 2Gbps de tráfico legítimo y al menos 6Gbps de trafico de capacidad de mitigación. El equipo debe soportar realizar crecimientos a través de licenciamiento adicional hasta una capacidad 5Gbps de tráfico legitimo.

	• La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2 y debe ser capaz de identificar y mitigar ataques de tipo volumétrico, agotamiento de estado y a nivel de aplicación. • La solución de mitigación de ataques DDoS debe proteger un canal de internet compuesto por dos (2) segmentos físicos en Fibra Optica de 10GE SR • La solución debe contar con un mecanismo de Bypass Externo. • La solución debe incluir interfaces de gestión (Management Ports) independeintes de los puertos de producción. • La solución de mitigación de ataques DDoS debe soportar IPv4 e IPv6 • La solución de DDoS ofertada debe ser "stateless", es decir, debe soportar un número ilimitado de sesiones concurrentes de ataque. • La solución de mitigación de ataques DDoS debe incluir doble fuente de poder "hot swappable" • La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de 2 Gbps • La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 5 Gbps • La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 6 Gbps • La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 5,5 Mpps • La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos. • La solución de mitigación de ataques DDoS debe incluir hardware dedicado para la mitigación de ataques SSL / TLS con capacidad de al menos 20KCPS con llaves RSA 2K FUNCIONALIDADES DE DETECCIÓN Y MITIGACIÓN DE ATAQUES La solución debe proteger contra al menos las siguientes anomalías de tráfico: ○ Checksum incorrecto de IPV4. ○ Tamaño de Cabecera capa invalido. ○ TTL igual a 0. ○ Cabecera IPV6 inconsistente. ○ Límites de salto IPV6 alcanzados. ○ Protocolo Capa 4 no soportado. ○ TCP flags invalido. ○ Tamaño de cabecera UDP invalido. ○ Dirección de origen o destino igual al Local Host. ○ Dirección de origen igual a la dirección de destino. ○ Puerto Capa 4 de origen o destino igual a cero. ○ Cebera de GRE invalida ○ Versión GRE Incorrecta Las políticas de seguridad se podrán configurar en modo reporte o en modo bloqueo La solución debe contar con análisis de comportamiento de red para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos las siguientes inundaciones de tráfico: ○ Inundación de red UDP. ○ Inundación de red ICMP. ○ Inundación de red IGMP. ○ Inundación de red TCP con flag SYN. ○ Inundación de red TCP con flag RST. ○ Inundación de red TCP con flag ACK.

	○ Inundación de red TCP con flag PSH. ○ Inundación de red TCP con flag FIN. ○ Inundación de red TCP con flag SYN y ACK. ○ Inundación de red TCP flag FRAG. ○ Inundación de red UDP con flag FRAG. • La solución debe aprender acerca del tráfico y configurar automáticamente las líneas base de tráfico y thresholds de ataques. • La solución debe correlacionar parámetros que varíen con la tasa de tráfico con parámetros que no varíen con la tasa de tráfico para determinar la condición de ataque. • La solución debe incluir un mecanismo preciso de detección de inundaciones UDP que tenga en cuenta parámetros que varíen con la tasa de tráfico y parámetros que no varíen con la tasa de tráfico, incluyendo: ○ Ancho de banda UDP. ○ Tasa de paquetes por segundo. ○ Tasa de conexiones por segundo. • La solución debe crear y aplicar automáticamente (sin intervención humana) y en tiempo real una firma para detener los ataques de “día cero” en capa de red. • La solución debe proteger contra ataques de tipo ráfaga (burst attacks) identificando que una nueva ráfaga de tráfico pertenece a una firma en tiempo real previamente creada. • La solución debe incluir protección contra ataques DDoS de inundación de paquetes fuera de estado. • La solución debe incluir protección contra ataques DDoS de tipo SYN Flood • La protección contra ataques SYN Flood a través del seguimiento de paquetes SYN enviados a cada IP Destino y Puerto. • La protección de SYN Flood debe prevenir contra ataques de tipo Spoofed-SYN-flood que vayan dirigidos a múltiples puertos destinos, a través del seguimiento de paquetes SYN enviados a toda la red configurada en la política. • La protección de SYN Flood debe contar con al menos dos métodos de autenticación TCP: ACK Fuera de Secuencia y Proxy Transparente • La protección de SYN Flood, para los protocolos http y https, debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script • La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, MX, PTR, Test, SOA, NAPTR, SRV, Other • La solución debe mitigar inundaciones de DNS recursivas (inundaciones de dominios aleatorios) bloqueando el tráfico que haga match con la firma en tiempo real creada, mientras permite el tráfico en la lista de FQDNs aprendida. • La protección de ataques DDoS DNS debe mitigar ataques de tipo amplificación o reflexión de DNS • La protección de ataques DDoS DNS debe mitigar ataques de tipo Brute Force de DNS • La solución de mitigación de ataques DDoS debe proteger contra ataques HTTPS Floods • La protección contra ataques HTTPS debe soportar las siguientes versiones del protocolo SSL usando hardware dedicado: SSL 3.0, TLS1.0, TLS 1.1, TLS 1.2 y TLS 1.3 • La protección contra ataques HTTPS debe permitir importar los certificados digitales y asociarlos a los servidores HTTPS protegidos.

	• La protección contra ataques HTTPS debe permitir asignar varios certificados a un objeto protegido y elegir el certificado vía SNI. • La protección contra ataques HTTPS Flood debe funcionar a través de análisis de comportamiento del tráfico hacia los servidores HTTPS. • La protección contra ataques HTTPS Flood debe aprender y configurar automáticamente las líneas base y thresholds de ataques sobre cada servidor configurado. • La protección contra ataques HTTPS Flood debe correlacionar parámetros que varíen con la tasa de tráfico con parámetros que no varíen para determinar la condición de ataque HTTPS Flood. • La solución debe ser capaz de detectar ataques en HTTPS sin necesidad de descifrar el tráfico previamente. • La protección contra ataques HTTPS Flood debe funcionar solo con el tráfico de entrante (Ingress-Only o Inbound). • La protección contra ataques HTTPS flood debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script • La protección contra ataques HTTPS flood debe identificar automáticamente una lista de IP origen sospechosas del ataque. • La protección contra ataques HTTPS Flood debe contar con al menos los siguientes métodos de mitigación: o Mitigación del primer request de los fuentes/orígenes sospechosos haciendo autenticación HTTPS únicamente a las fuentes/orígenes sospechosos o Limitar la tasa de tráfico a los orígenes sospechosos o Mitigación del primer request de todas las fuentes/orígenes haciendo autenticación HTTPS a todos los orígenes que se conecten a los servidores protegidos. • La protección contra ataques HTTPS Flood debe soportar Inspección selectiva completa por cada objeto (servidor) protegido, de tal que forma que el tráfico desencriptado después sea pasado por módulos adicionales de mitigación. • La protección contra ataques HTTPS Flood podrá anidar distintos métodos de mitigación y dichos métodos escalarán automáticamente en caso de que el ataque no esté siendo mitigado. • La solución debe permitir crear reglas de listas negras y listas blancas, incluyendo al menos los siguientes parámetros de clasificación: o Red Origen o Puerto Origen o Red Destino o Puerto Desinto o Protocolo • La solución de mitigación de ataques DDoS debe incluir un mecanismo de protección contra escaneos de puertos TCP, UDP e ICMP • La protección contra escaneos debe funcionar a través de análisis de comportamiento y el nivel de sensitividad de la protección debe ser configurado por el operador. • La protección contra escaneos debe tener la capacidad de crear listas blancas de direcciones IP origen y puertos • La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado. • La solución de mitigación de ataques DDoS debe incluir una protección basada en firmas de ataques conocidos que permita al menos mitigar los siguientes tipos de ataques: o Inundaciones TCP, UDPe ICMP conocidas o Herramientas de ataques conocidas disponibles en Internet o Inundaciones de ataques conocidos creados por bots

	○ Vulnerabilidades en los servidores: Web, Mail, FTP, SQL, DNS, SIP ○ Troyanos y backdoors ○ Gusanos y Virus ○ IRC Bots ○ Spyware ○ Phishing ○ Anonymizers • La protección basada en firmas de ataques conocidos debe incluir grupos de firmas preconfigurados para ser aplicados en las políticas. • La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas. • La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización • La protección de geolocalización debe permitir la configuración de un perfil de bloqueo por países y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas. • La solución de mitigación de ataques DDoS debe incluir una lista de IP de mala reputación productos del centro de investigación del fabricante, que será actualizada periódicamente. • Para cada una de las categorías listadas se podrá configurar al menos las siguientes acciones: Bloqueo, Bloqueo y Reporte, Bypass. • La lista de IP maliciosas, en conjunto con las acciones configuradas por categorías, debe aplicarse sobre cada política de seguridad. • El oferente debe presentar carta emitida por el fabricante de la solución ofertada en donde confirme que es partner autorizado para el suministro, instalación y soporte de los equipos que hacen parte de la solución y el cumplimiento del 100% de los requerimientos técnicos detallados en el presente documento. • Los servicios profesiones de implementación deben ser avalados presentando carta del fabricante de la solución ofertada.
APPLIANCE ANTISPAM	Servicio de Appliance que ofrece revisión de correo electrónico entrante y saliente de manera continua con protección multicapa contra todo el espectro de amenazas del correo electrónico, que permita prevenir, detectar y responder a las amenazas del correo electrónico incluyendo spam, phishing, malware día cero, suplantación de identidad y ataques Business Email Compromise. La solución deberá contar como mínimo con las siguientes funcionalidades: • Protección contra las amenazas de correo electrónico antispam y antimalware con técnicas avanzadas como protección contra brotes, desarme y reconstrucción de contenidos, análisis de sandbox, detección de suplantación y otras tecnologías para detener el correo masivo no deseado, el phishing, el ransomware el correo electrónico comercial comprometido y los ataques selectivos. • Debe soportar integración con la plataforma de Sandbox del SOC de la entidad, para la remisión de archivos sospechosos con el fin de ser analizados y detectar ataques de día cero. • Debe soportar integración nativa con la plataforma de SIEM del SOC de la entidad. • Debe soportar integración nativa con la plataforma de gestión de logs y reportes de seguridad de la entidad. • Debe soportar múltiples técnicas de inspección de remitentes, protocolos y contenidos protección de los usuarios del spam y correo basura.

	• Debe soportar el uso de una combinación de análisis de reputación, filtrado de conexiones, autenticación y verificación de destinatarios.
	• Debe realizar comprobaciones que incluyan IP, dominio, remitente, SPF, DKIM, DMARC y restricciones geográficas.
	• Debe soportar análisis de estructura y contenido de los mensajes en función de la firma digital, palabras clave, palabras clave en contexto, análisis de imágenes, URI incrustadas y análisis del comportamiento y la protección contra brotes de spam.
	• Debe soportar tecnologías estáticas y dinámicas que incluyan firmas, heurística y comportamiento junto con la prevención de brotes de virus y detección sofisticada de spoof.
	• Debe soportar Dashboards en tiempo real, presentando informes detallados, cuarentena centralizada y los controles de usuario de fácil utilización.
	• Debe soportar una interfaz de usuario intuitiva combinada con funciones flexibles de MTA y gestión del correo.
	• Debe soportar visibilidad y un control total del tráfico de correo electrónico.
	• Debe soportar servicios de agente de transferencia de correo (MTA) proxy entrante y saliente (MTA) para las pasarelas de correo electrónico existentes.
	• Debe soportar un modo Gateway mediante el cual un cambio en registro MX del DNS redirija el correo electrónico al appliance para realizar el análisis.
	• Debe soportar funciones de servidor de mensajería independiente con funcionalidad completa de servidor de correo SMTP, incluyendo soporte para acceso seguro POP3, IMAP y WebMail.
	• Debe soportar las siguientes características del Sistema:
	  ○ Despliegue Onpremise o en una nube pública o privada
	  ○ Pasarela, API M365, transparente y modo servidor
	  ○ Inspección de entrada y salida
	  ○ Compatibilidad con varios dominios de correo electrónico con personalización por dominio.
	  ○ Soporte MSSP multi-tenant con soporte de marca blanca
	  ○ Administración multinivel
	  ○ Soporte de direcciones IPv4 e IPv6
	  ○ Alojamiento virtual mediante pools de direcciones IP de origen y/o destino
	  ○ Autenticación SMTP mediante LDAP, RADIUS, POP3 e IMAP
	  ○ Enrutamiento de correo electrónico basado en LDAP
	  ○ Inspección por usuario mediante atributos LDAP por política (dominio)
	  ○ Política basada en la ubicación geográfica IP
	  ○ Interfaz de Webmail para implementaciones en modo servidor y gestión de cuarentena
	  ○ Gestión de colas de correo
	  ○ Compatibilidad con varios idiomas para Webmail y la interfaz de administración
	  ○ Cumplimiento de SMTP RFC
	  ○ Interfaz Gráfica de Usuario GUI HTML 5
	  ○ Compatibilidad con servicios en la nube como Microsoft 365, Google Workspace, Amazon AWS y Microsoft Azure.
	• Debe soportar las siguientes características del Antispam
	  ○ Reputación de remitentes y dominios
	  ○ Firmas de spam y archivos adjuntos
	  ○ Reglas heurísticas dinámicas

	○ Protección contra brotes ○ Filtrado completo de categorías de URL de spam, malware y phishing ○ Filtrado completo de categorías de URL pornográficas y para adultos ○ Filtrado completo de categorías de URL dominios recién registrados ○ Listas grises para direcciones IPv4, IPv6 y cuentas de correo electrónico ○ Reputación local de remitentes (basada en IPv4, IPv6 y End Point ID) ○ Análisis de comportamiento ○ Integración con URI de spam de terceros y listas negras en tiempo real (SURBL/RBL) ○ Detección de boletines (greymail) y boletines sospechosos ○ Escaneado de PDF y análisis de imágenes ○ Listas de bloqueo/seguridad a nivel global, de dominio y de usuario ○ Compatibilidad con estándares de identidad de remitentes empresariales ○ Marco de política de remitentes (SPF) ○ Correo identificado por claves de dominio (DKIM) ○ Autenticación de mensajes basada en dominios (DMARC) ○ Perfiles flexibles de acción y notificación ○ Múltiples cuarentenas de autoservicio por sistema y por usuario • Debe soportar protección contra ataques selectivos ○ Debe soportar eliminación de macros y contenido activo en archivos adjuntos en documentos Office y PDF ○ Debe soportar eliminación de eliminación del contenido HTML del correo electrónico mediante la eliminación de hipervínculos y la reescritura de URL. ○ Debe soportar compromiso del correo electrónico empresarial (BEC) ○ Protección antispoof multinivel ○ Análisis de suplantación: detección manual y automática de suplantación de direcciones ○ Detección de dominios primos ○ URL Click Protect para reescribir URLs y volver a escanear en el acceso • Debe soportar Integración API ○ Integración de correo electrónico de Microsoft 365 ○ Recuperación de amenazas posterior a la entrega ○ Escaneo programado ○ Escaneo en tiempo real ○ Escaneo de correo interno • Debe soportar detección de contenidos ○ Comprobación de firmas CPRL ○ Detección de comportamiento basada en heurística ○ Detección de greyware ○ Servicio de protección frente a brotes de virus ○ Inteligencia global sobre amenazas y análisis de datos ○ Detección de contenido activo (PDF y documentos de Office) ○ Reescaneado de amenazas al liberar la cuarentena ○ Comprobación personalizada de hash de archivos ○ Detección de tipo de archivo y MIME

	○ Prevención integral de la pérdida de datos con detección de huellas dactilares de archivos y datos confidenciales ○ Huella digital automática de archivos compartidos de Windows y de carga manual ○ Detección de información sanitaria, financiera, de identificación personal y blasfemia. ○ Descifrado automático de archivos, PDF y documentos de Office mediante listas de contraseñas integradas y definidas por el administrador, así como de palabras. ○ Listas de contraseñas incorporadas y definidas por el administrador y detección de palabras en el cuerpo del correo electrónico ○ Identificación sobre contenido ilícito y sexualmente explícito. • Debe soportar Encriptación ○ Amplio soporte de cifrado ○ TLS de servidor a servidor con control de cifrado granular y aplicación opcional ○ S/MIME ○ Cifrado sin cliente en el escritorio del destinatario mediante cifrado basado en la identidad (IBE) ○ Complemento opcional de Outlook para activar el cifrado basado en la identidad (IBE) • Debe soportar Gestión, registro e Informes ○ Modos de gestión básico/avanzado ○ Cuentas de administración por dominio basadas en funciones ○ Registro e informes exhaustivos de actividades, cambios de configuración e incidencias ○ Módulo de informes integrado ○ Seguimiento detallado de mensajes ○ Cuarentena centralizada para despliegues a gran escala ○ Soporte SNMP mediante MIB estándar y privada con traps basados en umbrales ○ Soporte de servidor de almacenamiento local o externo, incluyendo dispositivos iSCSI ○ Compatibilidad con Syslog externo ○ API REST abierta para configuración y gestión • Debe soportar alta Disponibilidad HA ○ Alta disponibilidad admitida en todos los escenarios de implantación ○ Modo activo-pasivo ○ Modo de sincronización de configuración Activo-Activo ○ Sincronización de cuarentena y cola de correo ○ Detección y notificación de fallos de dispositivos ○ Soporte de estado de enlace, conmutación por error e interfaz redundante • El Appliance debe contar como mínimo con las siguientes especificaciones ○ Puertos RJ-45 10/100/1000: 4 ○ Storage 2 x 1 TB ○ RAID Storage Management: Software 0, 1 ○ Factor de Forma: Rack Mount, 1U ○ Módulo TPM: Si ○ Dominios de Email protegidos: 70 ○ Políticas basadas en destinatarios (por dominio / por sistema) Entrante o saliente: 400 / 1500 ○ Buzones de correo en modo servidor: 400

	○ Antispam, antivirus, autenticación y Perfiles de contenido (por dominio / por sistema): 50/200 ○ Data Loss Prevention: SI ○ Cuarentena Centralizada: SI ○ Enrutamiento de Email: 250.000 emails por hora ○ Protección Antispam + Brote de Virus: 200.000 emails por hora • El proveedor deberá suministrar todos los elementos (fibras, cables, transceivers, etc, necesarios para hacer funcional la solución)
RENOVACIÓN DE SUSCRIPCIÓN LACNIC DIRECCIONAMIENTO IPV6	a. Realizar los trámites técnicos, administrativos y financieros ante LACNIC que sean necesarios para la renovación de la membresía y bloque de direcciones IPv6 por tres (3) años a nombre del DANE. b. Acompañar a la Entidad en la validación técnica que se requiera para la entrega de información, asistencia y cooperación que LACNIC solicite durante el proceso de asignación del bloque de direccionamiento. c. Entregar la documentación técnica, administrativa que demuestre el cumplimiento de este requerimiento contractual, incluidos los comprobantes de pago efectuados a LACNIC dónde se evidencie que los trámites se hacen a nombre del DANE. d. Entregar a nombre del DANE la membresía otorgada por LACNIC en completo registro, con vigencia de tres (3) años.

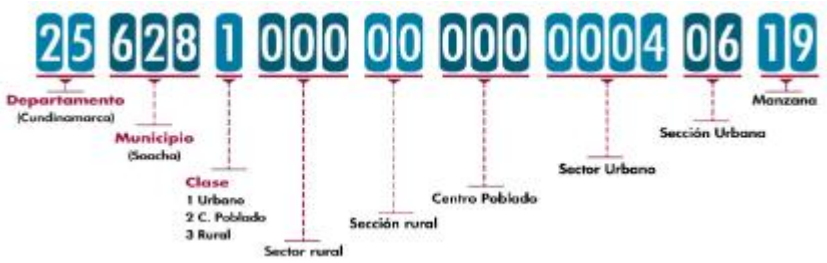
2 ENLACES DEDICADOS PUNTO A PUNTO CENTROS OPERATIVOS MUNICIPALES

CENTROS OPERATIVOS MUNICIPALES	Los centros operativos municipales (COM) son espacios donde se desarrollan actividades de carácter operativo del Censo Económico Nacional Urbano. Estos espacios requieren contar con el servicio de conectividad para las labores operativas y de transmisión de información hacia y desde la sede del nivel central del DANE en la ciudad de Bogotá. De la misma forma estos centros operativos municipales (COM) accederán a internet de manera controlada a través de un canal de internet dedicado que desbordará desde la sede del nivel central del DANE en la ciudad de Bogotá los cuales se deberán integrar con la solución de Firewall perimetral de la Entidad, y permitir la integración de los Access points instalados en los Centros Operativos Municipales con la controladora Inalámbrica que se especifican en la solución de red inalámbrica en el presente anexo técnico. **NOTA:** Esta es una red independiente de la red de las sedes del DANE a nivel nacional.
UBICACIÓN DE LOS CENTROS OPERATIVOS MUNICIPALES (COM)	Se suministran los insumos para que los proveedores de servicios de internet (ISP) puedan identificar las generalidades de las ubicaciones de las sedes y llevar a cabo sus evaluaciones de factibilidad, basándose en los siguientes criterios: **A. Centros Operativos Municipales con dirección Actual** Algunos de estos Centros Operativos Municipales - COM está ubicados en sedes actuales del DANE y en otros casos en sedes temporales que se tienen actualmente en los diferentes municipios donde se aplicará el censo. Para estos dos casos se tienen direcciones específicas que se presentan en el listado de sitios. **B. Centros Operativos Municipales con código Divipola**

Para otros Centros Operativos Municipales - COM en lugar de una dirección se cuenta el código de la Divipola https://www.datos.gov.co/widgets/gdxc-w37w Este es código jerárquico que va desde el nivel más amplio (código del departamento) hasta el nivel más detallado (código de la manzana censal en el área urbana y código de la sección rural en el área rural del municipio). Está compuesto por 22 posiciones o campos que se describen y se ilustran a continuación con un ejemplo:

- Posición 1 y 2: Departamento
- Posición 3 a 5: Municipio
- Posición 6: Clase (Urbano = 1, Centro poblado = 2 y Área rural dispersa= 3)
- Posición 7 a 9: Sector rural
- Posición 10 y 11: Sección rural
- Posición 12 a 14: Código del centro poblado
- Posición 15 a 18: Sector urbano
- Posición 19 y 20: Sección urbana
- Posición 21 y 22: Manzana censal

Ejemplo:

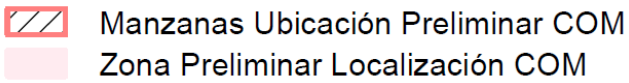


C. Centros Operativos Municipales con planchas cartográficas

Se han desarrollado ubicaciones preliminares para los Centros Operativos Municipales - COM que aún no cuentan con una sede específica. Estas ubicaciones están determinadas en áreas específicas que se detallan en una serie de planchas cartográficas que contienen:

- Departamento
- Municipio
- Manzana o polígono
- Latitud y longitud del polígono

Cada municipio tiene un mapa en el cual se indica mediante las siguientes convenciones la posible ubicación del COM:



Ver (Anexo Mapas Municipios)

D. Centros Operativos Municipales con planchas cartográficas

Teniendo en cuenta la posible ubicación de los Centros Operativos Municipales – COM, se generó una capa geográfica en formato shapefile, denominada AREAS.zip. Para su visualización, se sugiere hacer uso de la plataforma

	desarrollada por el Instituto Geográfico Agustín Codazzi – IGAC denominada Colombia en Mapas, https://www.colombiaenmapas.gov.co, la cual permite la consulta de servicios web geográficos mediante la cual se podrán consultar las coordenadas respectivas. *Ver (Instructivo áreas COM y AREAS.zip)* https://drive.google.com/drive/folders/1oMVpercGJmvn5sQJe0l-zSew_z--KGJ6?usp=sharing **NOTA:** Se informa a los ISP que se estima que puede llegarse a dar un cambio en las sedes de los COM dado que desde ahora y hasta el momento en que se requiere la sede para ser utilizada por el Censo (marzo - abril del 2024) se pueden presentar cambios pues los sitios se gestionaron con administraciones públicas salientes (alcaldías/gobernaciones). La variabilidad debe ser mínima si se considera que los sitios se buscan en la cabecera municipal y las zonas céntricas de estos municipios. Se solicita que se identifiquen las ubicaciones por cualquiera de las metodologías indicadas y se establezca la viabilidad técnica y costo para poder presentar una oferta para estas sedes sin tener que contar con una ubicación exacta.

Los enlaces a suministrar se listan a continuación y se presentan las características solicitadas para cada uno de ellos:

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
1	BOGOTA	BOGOTA	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	Enlaces de Conectividad Terrestre	Enlaces Dedicados a Internet	1.5Gbps	1.5Gbps	1:1	8	Zona 1
2	BOGOTA	BOGOTA	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	1.5Gbps	1.5Gbps	1:1	8	Zona 1
3	CALDAS	MANIZALES 1	Cámara de Comercio - Cra. 23 No. 26-60	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
4	TOLIMA	ESPINAL	Cámara de Comercio del Sur y Oriente del Tolima - Cra. 12 No. 12-20, Barrio Caballero y Gongora	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
5	RISARALDA	PEREIRA	CED Ormaza - Cra. 3 bis No. 5- 38 Avenida del Rio	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
6	TOLIMA	IBAGUE 1	Cra. 4 No. 10-77, Barrio Centro, Edificio Centro Empresarial	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
7	RISARALDA	SANTA ROSA DE CABAL	Unisarc - Kilometro 4 vía Santa Rosa de Cabal - Chinchina	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
8	RISARALDA	DOSQUEBRADAS	66170100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
9	QUINDIO	ARMENIA 1	63001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
10	QUINDIO	ARMENIA 2	63001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
11	CALDAS	MANIZALES 2	17001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
12	CALDAS	LA DORADA	17380100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
13	TOLIMA	IBAGUE 2	73001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
14	TOLIMA	IBAGUE 3	73001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
15	TOLIMA	IBAGUE 4	73001100000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
16	BOGOTA	BOGOTA	Calle 64G No. 92-56, Barrio Álamos Industrial	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	128Mbps	128Mbps	1:1	8	Zona 1
17	CAQUETA	FLORENCIA	Calle 24 No. 4A - 49, Barrio la Libertad.	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
18	HUILA	NEIVA	Calle 18 No. 7-75, Barrio Quirinal.	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
19	GUAVIARE	SAN JOSÉ DEL GUAVIARE	Calle 5A No. 27 - 16, Barrio 20 de Julio.	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
20	META	VILLAVICENCIO	Carrera 43D No. 16-06, Barrio El Buque	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 1
21	CASANARE	YOPAL	Transversal 18 Nº 7 - 05, Piso 4.	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2
22	AMAZONAS	LETICIA	Carrera 7 No. 6-104	Enlaces de Conectividad Satelital	Enlaces Dedicados entre Puntos MPLS	8Mbps	4Mbps	1:1	8	Zona 4
23	META	ACACIAS	5000610000000000010606 - 5000610000000000020420 - 5000610000000000040313	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
24	META	GRANADA	5031310000000000010503 - 5031310000000000010706 - 5031310000000000010502	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
25	BOYACÁ	TUNJA	Calle 48 A No. 1 - 70 Este . Barrio Lirio Real	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
26	BOYACÁ	CHIQUINQUIRA	1517610000000000020212 - 1517610000000000010907 - 1517610000000000010513	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
27	BOYACÁ	SOGAMOSO	1575910000000000060118 - 1575910000000000060103 - 1575910000000000060214	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
28	BOYACÁ	DUITAMA	1523810000000000040202 - 1523810000000000040102 - 1523810000000000020303	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
29	HUILA	GARZON	4129810000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
30	HUILA	PITALITO	4155110000000000030430 - 4155110000000000010302	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
31	CUNDINAMARCA	ZIPAQUIRA	2589910000000000030414 - 2589910000000000040203 - 2589910000000000040949	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
32	CUNDINAMARCA	CAJICA	2512620010101100000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
33	CUNDINAMARCA	CHIA	2517510000000000010514 - 2517510000000000020628	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
34	CUNDINAMARCA	FACATATIVÁ	2526910000000000010412 - 2526910000000000020608 - 2526910000000000020614	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
35	CUNDINAMARCA	MADRID	2543010000000000010606 - 2543010000000000010516	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
36	CUNDINAMARCA	FUSAGASUGÁ	2529010000000000040118 - 2529010000000000040111 - 2529010000000000040113	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
37	CUNDINAMARCA	GIRARDOT	2530710000000000210109 - 2530710000000000100313 - 2530710000000000200103	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
38	CUNDINAMARCA	FUNZA	2528610000000000020637 - 2528610000000000010712 - 2528610000000000010148	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
39	CUNDINAMARCA	MOSQUERA	2547310000000000010412 - 2547310000000000020426	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
40	CUNDINAMARCA	SOACHA	2575410000000000030107 - 2575410000000000020928 - 2575410000000000020307 - 257541000000000020205	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
41	CORDOBA	SAHAGUN	2366010000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
42	CORDOBA	CERETÉ	2316210000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
43	CORDOBA	LORICA	2341710000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
44	CORDOBA	MONTERIA	2300110000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
45	CORDOBA	PLANETA RICA	2355510000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
46	CORDOBA	MONTELIBANO	2346610000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
47	ANTIOQUIA	MEDELLÍN 1	500110000000005000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
48	ANTIOQUIA	MEDELLÍN 2	500110000000010000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
49	ANTIOQUIA	MEDELLÍN 3	500110000000010000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
50	ANTIOQUIA	MEDELLÍN 4	500110000000015000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
51	ANTIOQUIA	APARTADÓ	504520020300900000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
52	ANTIOQUIA	TURBO	583710000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
53	ANTIOQUIA	CAUCASIA	515410000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
54	ANTIOQUIA	SABANETA	563110000000090000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
55	ANTIOQUIA	ITAGUI	563110000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
56	ANTIOQUIA	BELLO	508810000000052000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
57	ANTIOQUIA	RIONEGRO	561510000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
58	ANTIOQUIA	CALDAS	512910000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
59	ANTIOQUIA	ENVIGADO	512910000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
60	CHOCO	QUIBDÓ	2700110000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
61	ARAUCA	ARAUCA	Carrera 24 entre calle 18 y 19 Barrio la esperanza	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
62	ARAUCA	ARAUQUITA	Calle 4 # 7-36 Barrio Charalá	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 4
63	ARAUCA	SARAVENA	Carrera 15 # 23-03 Barrio Centro	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
64	SANTANDER	BARBOSA	Carrera 9 # 7-15	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
65	SANTANDER	BARRANCABERMEJA	Transversal 49A # 10-101 Barrio el comercio	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
66	SANTANDER	BUCARAMANGA	Calle 20 26-27	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 1
67	SANTANDER	FLORIDABLANCA	Avenida 33 # 117-100 Barrio Nuevo Villabel	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
68	SANTANDER	SAN GIL	Oficina esquina del Águila segundo piso parque principal- oficina en arriendo- Carrera 10 # 13-17	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
69	NORTE DE SANTANDER	CÚCUTA	Sede DANE- Calle 9 # 9E- 100 Barrio la Riviera	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 2
70	NORTE DE SANTANDER	LOS PATIOS	Centro del adulto mayor- Avenida 0 # 34-35 Barrio 12 de Octubre	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
71	NORTE DE SANTANDER	OCAÑA	Centro de empleo y emprendimiento - Carrera 40 # 7-34 Barrio la Gloria	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
72	NORTE DE SANTANDER	PAMPLONA	Institución educativa san francisco de Asís - Carrera 6 # 1B- 71	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
73	NORTE DE SANTANDER	TIBÚ	Centro de convivencia ciudadana- Carrera 5 # 4A-34 Barrio Miraflores	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 4
74	NORTE DE SANTANDER	VILLA DEL ROSARIO	Sede SENA Villa del Rosario - Calle 4 # 4-28 Barrio Fátima	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
75	ARAUCA	TAME	8179410000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
76	SANTANDER	GIRÓN	8179410000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
77	SANTANDER	PIEDECUESTA	6830710000000000000000	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
78	VALLE DEL CAUCA	BUENAVENTURA	Calle 5 # 18-24 (universidad del Valle Buenaventura)	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
79	VALLE DEL CAUCA	CALI 1	CRA 28F # 72L - 79 BARRIO EL POBLADO I - CENTRO DE SERVICIO FUNDACION CARVAJAL	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
80	VALLE DEL CAUCA	CALI 2	CASA COMUNAL BARRIO EL NACIONAL: CRA 18 # 7 - 500	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
81	VALLE DEL CAUCA	CALI 3	CARRERA 37A # 23-01 BARRIO CRISTOBAL COLON	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
82	VALLE DEL CAUCA	CALI 4	CALLE 2 # 12 A 50	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
83	VALLE DEL CAUCA	CANDELARIA	CALLE 12 # 14-22 BARRIO BELEN-VILLA GORGONA	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 4
84	VALLE DEL CAUCA	CARTAGO	FENALCO CALLE 12 # 3 - 66 OF 205	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
85	VALLE DEL CAUCA	EL CERRITO	Sede del I.E. Jorge Isaac, ubicada en la Calle 8 Carrera 1A - 5A	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 4
86	VALLE DEL CAUCA	FLORIDA	CALLE 11 # 9-10 BARRIO CIUDADELA DON PACO	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
87	VALLE DEL CAUCA	GUADALAJARA DE BUGA	Calle 1 Sur # 18-06	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
88	VALLE DEL CAUCA	JAMUNDÍ	Calle 9 # 17 - 04, Carrera 11 # 15 - 141	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
89	VALLE DEL CAUCA	PALMIRA	CALLE 54 # 26-40 BARRIO LAS MERCEDES	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
90	VALLE DEL CAUCA	PRADERA	CARRERA 8 CON CALLE 8 ESQUINA # 7-65	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
91	VALLE DEL CAUCA	TULUÁ	FENALCO CRA 36 # 31 - 35	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2
92	VALLE DEL CAUCA	YUMBO	Calle 8 # 13 – 19, Barrio Buenos Aires	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
93	PUTUMAYO	MOCOA	Sede ITP, INSTITUTO TECNOLOGICO DEL PUTUMAYO, Sede Aire Libre, Br. Luis Carlos Galán, Calle 17, Carrera 17	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
94	PUTUMAYO	PUERTO ASÍS	Edificio CAM, Calle 10 cra 19 Esquina, Centro	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
95	NARIÑO	IPIALES	CRA. 9 # 6-36 IE. ALFONSO LOPEZ, BARRIO ALFONSO LOPEZ	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
96	NARIÑO	PASTO	CRA. 6 ESTE # 18-58 INSTALACIONES CANCHA DEPORTIVA BARRIO EL TEJAR	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2
97	NARIÑO	SAN ANDRÉS DE TUMACO	CALLE SUCRE No 19-32 BARRIO CENTRO	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
98	CAUCA	POPAYÁN	CR 6 Puente Viejo Cauca, Colegio Gabriela Mistral	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2
99	CAUCA	SANTANDER DE QUILICHAO	CALLE 4 #8-40 CENTRO SANTANDER DE QUILICHAO	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
100	ATLANTICO	BARRANQUILLA	Carrera 58 No. 70 - 93 (IGAC)	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 1
101	ATLANTICO	MALAMBO	Cra. 16 10-24 esquina	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
102	ATLANTICO	SABANALARGA	Sede regional Centro Sabanalarga CLL 6 26B-01	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
103	ATLANTICO	SOLEDAD	El Nodo Sena Soledad_ KR 24 Av el platanal_ Centro Comercial Carnaval	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1
104	BOLIVAR	CARTAGENA	Transversal 54 # 28 25 barrio bosque	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 1
105	BOLIVAR	MAGANGUÉ	Barrio centro calle 11 carrera 2 y 3 antigua sede alcaldía	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
106	BOLIVAR	TURBACO	Barrio la granja antigua carretera ferrocarril centro de vida Eugenia Arrazola, calle 35	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 1
107	GUAJIRA	MAICAO	Calle 11 No.20 -45 Barrio El Carmen Centro de Atención Social	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
108	GUAJIRA	RIOHACHA	Avenida los estudiantes cra 15 #1-40	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 3
109	SAN ANDRES	SAN ANDRÉS	Avenida Francisco Newball No. 9-184	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
110	MAGDALENA	CIÉNAGA	Cra. 20 No. 5B-23	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
111	MAGDALENA	EL BANCO	Calle 7 - Carrera 12- Esquina- Centro cultural Montesori	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 3
112	MAGDALENA	SANTA MARTA	Calle 17A 9-104 sede DANE	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	25Mbps	25Mbps	1:1	8	Zona 1

ID	DPTO	MUNICIPIO	DIRECCIÓN / CÓDIGO DANE (Manzana)	Categoría	Nombre del servicio	BW download	BW upload	Re-USO	Tiempo Meses	Zona
113	SUCRE	SINCELEJO	Calle 18 No. 10-100 Barrio Kennedy	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 2
114	CESAR	AGUACHICA	Calle 11 No. 11-53	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	10Mbps	10Mbps	1:1	8	Zona 2
115	CESAR	VALLEDUPAR	Transversal 19 con Diagonal 18a barrio sábanas	Enlaces de Conectividad Terrestre	Enlaces Dedicados entre Puntos MPLS	20Mbps	20Mbps	1:1	8	Zona 1

GENERALIDADES	Se requiere una solución de enlaces de conectividad que comunique los Centros Operativos Municipales del DANE a nivel nacional con la sede del nivel central en la ciudad de Bogotá. Su objetivo es transmisión de datos y/o acceso a Internet a centralizado a través del canal de internet de este servicio ubicado en la sede principal para soportar las actividades del Censo Económico Nacional. Los enlaces dedicados podrán ser implementados en diferentes tecnologías de Red de última milla, dependiendo de los anchos de banda requeridos, donde se deberán priorizar los medios terrestres como fibra óptica, radio enlace o cobre donde sea necesaria su utilización. El Proveedor debe suministrar el servicio utilizando la mejor tecnología disponible de manera que le permita cumplir los ANS y características técnicas definidas en esta ficha técnica. La conectividad física para el total de sedes remotas y sede principal del DANE deberá estar provista de elementos para garantizar la operatividad del servicio, es decir implementar un enlace MPLS en las sedes remotas, doble enlace de conectividad a la sede principal del DANE haciendo uso de canales con medio de transporte en fibra óptica, radioenlaces licenciados y satelitales. Para brindar al DANE el mayor nivel de eficiencia y disponibilidad en la continuidad del servicio y en la calidad de la comunicación. En caso de instalación de radio enlaces, estos deberán ser radio enlaces licenciados, no se aceptan radio enlaces no licenciados. Todos los servicios de enlaces de conectividad deberán prestarse sin reúso. Para los enlaces de Internet dedicado, el proveedor debe garantizar acceso internacional mínimo el 100% del ancho de banda del enlace contratado. El Proveedor debe suministrar el servicio utilizando equipos que le permitan cumplir los ANS y características técnicas definidas en la presente ficha técnica. • Se requiere una red MPLS que conecte a todas los Centros Operativos Municipales con la sede principal y viceversa. • Se requieren canales sin reúso, incluyendo elementos y configuraciones que permitan su operación las 24 horas del día. • Se requiere un canal de Internet para instalar en la sede principal del DANE en Bogotá Mínimo de 1.5Gbps. • Se requiere un canal de MPLS para instalar en la sede principal del DANE en la ciudad de Bogotá mínimo de 1.5 Gbps.

	• La Disponibilidad del canal de internet en la sede principal del DANE debe ser de >=99.96% para canales con alta disponibilidad o redundancia y doble equipo CPE. • La disponibilidad del punto de concentración de la red MPLS en la sede principal del DANE debe ser de >=99.96% con última milla principal y backup y doble equipo CPE.
LATENCIA	Latencia: máximo 40ms
DISPONIBILIDAD EXIGIDA	La disponibilidad se mide usando la siguiente ecuación: $\left(1 - \frac{Número\ total\ de\ minutos\ en\ que\ el\ servico\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ contratados\ x\ 24\ horas\ x\ 60\ minutos}\right) x\ 100\%$ La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio de intercambio de datos sobre el enlace no está disponible, dividido en el número total de minutos en el mes facturado. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma individual sobre cada enlace. Es decir, **cada enlace debe cumplir con el valor exigido en el ANS**. **Disponibilidad exigida** Cada enlace deberá incluir un enlace MPLS (una última milla). La medición se hace teniendo en cuenta el único enlace que se tiene en cada una de las sedes remotas, es decir, la medición es por el enlace, en donde **cada enlace debe cumplir con el valor exigido en el ANS**. **Disponibilidad sedes remotas:** **Disponibilidad exigida >=99.6% mensual** **Penalidad por no conformidad - Descuento en facturación** • 98% <= disponibilidad < 99.6%: 10% de descuento sobre el costo este servicio. • 97% <= disponibilidad < 98%: 20% de descuento sobre el costo este servicio. • 95% <= disponibilidad < 97%: 50% de descuento sobre el costo este servicio. disponibilidad < 95%: 100% de descuento sobre el costo este servicio
RTO	El RTO por sus siglas en inglés es Recovery Time Objective o en español Tiempo Objetivo de Recuperación.

	El RTO es el tiempo máximo que el enlace puede estar fuera de servicio una vez se ha producido una Interrupción. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. En los casos en que la interrupción sea en la herramienta de monitoreo y no en el servicio; no se contabilizará la interrupción como parte del tiempo máximo que el servicio puede estar fuera de servicio. **RTO** **<= 8 minutos** **Penalidad por no conformidad - Descuento en facturación** • 8 min<RTO<=15 min: 10% de descuento sobre el costo total de este servicio. • 15 min<RTO<=25 min: 20% de descuento sobre el costo total de este servicio. • 25 min<RTO<=45 min: 50% de descuento sobre el costo total de este servicio. • 45 min<RTO: 100% de descuento sobre el costo total de este servicio.
INTERRUPCIONES MÁXIMAS	El ANS Interrupciones máximas hace referencia a el número máximo de Interrupciones durante el mes facturado. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace. La medición la debe hacer el proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo deben ser mantenidos por el proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. Esta información debe permitirle a la Entidad verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace teniendo en cuenta el único enlace que se tiene en cada una de las sedes remotas, es decir, la medición es por el enlace, en donde **cada enlace debe cumplir con el valor exigido en el ANS**. **Interrupciones máximas en un mes** 2 interrupciones **Penalidad por no conformidad - Descuento en facturación** • 3 interrupciones: 20% de descuento sobre el costo de este servicio. • 4 interrupciones: 50% de descuento sobre el costo de este servicio. • >5 Interrupciones: 100% de descuento sobre el costo de este servicio.

MTBF	El MTBF por sus siglas en inglés es Mean Time Between Failures o en español Tiempo Medio Entre Fallas. El MTBF es un indicador de confiabilidad definido como el promedio aritmético acumulado del tiempo entre Fallas asumiendo que el enlace se recupera de forma inmediata cuando se produce la Falla. Nota aclaratoria: El supuesto: “asumiendo que el servicio se recupera de forma inmediata” hace referencia a la forma en que se medirá en tiempo entre fallas y no a que necesariamente haya una recuperación instantánea de una falla. Una Falla se define como una degradación del servicio de conectividad con respecto a las condiciones pactadas en al Acuerdo Marco de Precios La medición la hace el Proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Proveedor para que puedan ser consultados por el DANE en cualquier momento durante la duración del servicio. La información mantenida por el Proveedor le debe permitir a la Entidad verificar el MTBF acumulado en cualquier momento durante la prestación del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. Nota aclaratoria: Una Falla es diferente a una Interrupción. La Falla está asociada a la confiabilidad del servicio y la Interrupción está asociada a la disponibilidad del servicio. **MTBF** >718 horas Penalidad por no conformidad - Descuento en facturación • 540 horas < MTBF <= 718 horas: 10% de descuento sobre el costo total de este servicio. • 360 horas < MTBF <= 540 horas: 20% de descuento sobre el costo total de este servicio. • 180 horas < MTBF <= 360 horas: 50% de descuento sobre el costo total de este servicio. • MTBF <= 180: 100% de descuento sobre el costo total de este servicio.
ANCHO DE BANDA	El ancho de banda corresponde al rango de frecuencias que ocupan los datos transmitidos por el enlace sin que se presente distorsión o pérdida de información. La medición la debe hacer el Proveedor una vez lo solicite el DANE por el tiempo y con la frecuencia que la Entidad lo requiera. Los resultados de la medición deben ser mantenidos por el Proveedor para que puedan ser consultadas por la Entidad durante la duración del servicio. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Ancho de banda** Debe ser igual o superior al ancho de banda contratado **Penalidad por no conformidad - Descuento en facturación** • Si se evidencia una reducción del 10% sobre el ancho de banda contratado: 40% de descuento sobre el costo del servicio

	• Si se evidencia una reducción del 20% sobre el ancho de banda contratado: 50% de descuento sobre el costo del servicio • Si se evidencia una reducción >= 30% sobre el ancho de banda contratado: 100% de descuento sobre el costo del servicio
CALIDAD Y OPORTUNIDAD EN LOS REPORTES ENTREGADOS	El Proveedor debe garantizar la calidad de la información que contienen los reportes que entrega a la Entidad. Con el fin de garantizar la calidad de los reportes se define el número máximo de devoluciones en que puede incurrir el Proveedor sin que se generen penalizaciones para cada nivel de servicio. Adicionalmente, se establecen las penalidades por no conformidad que se le harán al Proveedor cuando supera el número máximo de devoluciones. **Devoluciones máximas por cada reporte** <= 3 devoluciones de un mismo reporte **Penalidad por no conformidad - Descuento en facturación** • 4 devoluciones del mismo reporte: 10% • 5 devoluciones del mismo reporte: 20% • 6 devoluciones del mismo reporte: 50% • 7 devoluciones del mismo reporte: 100%
TIEMPO DE APROVISIONAMIENTO DE CRECIMIENTOS CONTEMPLADOS EN EL NIVEL DE ELASTICIDAD CONTRATADO	El crecimiento de los enlaces está dado por las características de elasticidad definidas en esta ficha. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Elasticidad alta** <= a 16 horas continuas **Penalidad por no conformidad - Descuento en facturación** • 2 horas continuas de retraso: 10% de descuento sobre el costo este servicio. • 4 horas continuas de retraso: 20% de descuento sobre el costo este servicio. • 6 horas continuas de retraso: 50% de descuento sobre el costo este servicio. 8 horas continuas de retraso: 100% de descuento sobre el costo este servicio.
EFECTIVIDAD EN RESOLUCIÓN DE INCIDENTES/SOLICITUDES	Aplicable para: • Solicitudes de cambios • Cambios en configuraciones • Habilitación de VPN. • Resolución de inquietudes • Entrega reportes e información. • Solución de incidentes La efectividad de resolución de solicitudes mide el tiempo máximo de solución de las solicitudes realizadas a la mesa de ayuda del Proveedor según su nivel de prioridad.

	El reloj que mide la efectividad de resolución comienza a contabilizar el tiempo desde el momento en que el ticket es registrado en la mesa de ayuda hasta que el Proveedor da una respuesta y soluciona el problema. Zona 1: • Prioridad 1: Efectividad de resolución <=4 horas • Prioridad 2: Efectividad de resolución <= 18 horas • Prioridad 3: Efectividad de resolución <= 64 horas Zona 2: • Prioridad 1: Efectividad de resolución <= 8 horas • Prioridad 2: Efectividad de resolución <= 32 horas • Prioridad 3: Efectividad de resolución <= 88 horas Zona 3 y 4: • Prioridad 1: Efectividad de resolución <= 20 horas • Prioridad 2: Efectividad de resolución <= 48 horas • Prioridad 3: Efectividad de resolución <= 112 horas
ELASTICIDAD	**Crecimiento definitivo** Ampliaciones definitivas en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. Una ampliación definitiva tiene una duración correspondiente al tiempo restante de servicio. Capacidad de crecimiento: Hasta el 100% sin cambio de equipos. **Crecimiento temporal** Ampliaciones en el ancho de banda que debe estar en capacidad de soportar el equipo inicialmente instalado. • Capacidad de crecimiento: Hasta el 100% sin cambio de equipos **Duración del crecimiento** • Mínima (días): Entre 7 días calendario hasta 30 días calendario • Máxima (mensual): 60 días calendario
HARDWARE Y SOFTWARE	El Proveedor debe garantizar toda la conectividad física y lógica requerida para la puesta en funcionamiento de los servicios y conectividad contratada. La conectividad física hace referencia a todos los elementos de hardware necesarios para proveer el servicio. (El DANE dispone de las condiciones de infraestructura para la entrega del servicio, tales como: energía regulada, sistema de puesta a tierra, rack y espacios de comunicaciones para instalar equipos de telecomunicaciones y condiciones ambientales óptimas para la temperatura de los equipos, esto en el caso que los servicios contratados así lo requieran). La conectividad lógica hace referencia a todos los elementos de software necesarios y su respectiva configuración para proveer el servicio.
NAP COLOMBIA	El ISP (Internet Service Provider) debe incluir conexión al NAP Colombia garantizando el 100% del ancho de banda contratado por parte de la Entidad compradora, garantizando que el tráfico de datos que tiene origen y destino en el territorio nacional no transite por enlaces internacionales y en conformidad a lo establecido en la Res. CRC 5078 de 2016 "Indicadores de Calidad" Res. 5050

	"compilada de las resoluciones de carácter general" y todas aquellas que adicionen, modifiquen o sustituyan.
REGISTRO TIC	El Proveedor para la prestación de los servicios de telecomunicaciones solicitados, deberá contar con el Registro TIC emitido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones el cual lo acredita como Proveedor de Redes y Servicios de Telecomunicaciones en el territorio nacional. EL Registro TIC deberá estar vigente durante toda la ejecución del contrato.
AISLAMIENTO DE RED	El Proveedor debe garantizar que el servicio de conectividad admite controles de aislamiento de red para tráfico entrante y saliente a través de métodos a nivel de capa 2 o 3. El Proveedor debe articular cualquier restricción, condición o requisito de red, como la traducción de dirección de red (NAT), la superposición de direcciones IP y controles de latencia para los procesos de traducción NAT
SERVICIO DE SOPORTE TÉCNICO	El Proveedor debe tener la capacidad de brindar servicio de soporte técnico remoto y en sitio para los servicios contratados por la Entidad. El Proveedor debe brindar soporte en sitio para evaluar y solucionar Fallas e Interrupciones que se presenten en los servicios contratados por la Entidad Compradora. El soporte será en sitio sólo en los casos en que no sea posible resolver el problema de forma remota. El servicio en sitio no significa costos adicionales para el DANE. Adicionalmente, el Proveedor debe brindar soporte remoto a nivel nacional a través de los siguientes canales: - Línea de atención telefónica gratuita con cobertura nacional. - Plataforma web para registro y monitoreo de tiquetes. - Correo electrónico. - Chat. El Proveedor debe garantizar que cuenta con un servicio de mesa de ayuda el cual deberá operar en instalaciones a cargo del proveedor. El Proveedor debe garantizar que exista un tiquete por cada reporte de Falla o Interrupción que haga el DANE. Los canales de soporte deben estar disponibles 7x24 durante el tiempo de ejecución del contrato. El grupo de soporte del Proveedor debe garantizar que los tickets: • Sean registrados, clasificados y asignados según su criticidad. • Sean resueltos en los tiempos acordados en los ANS. • Tengan un seguimiento adecuado. • Cumplan con esquemas de escalamiento definidos. Deben ser documentados con las respectivas evidencias y en caso de requerir atención en sitio anexar registros fotográficos donde se observe Georreferenciación, fecha y hora donde ocurrió el evento.
SERVICIO DE SOPORTE TÉCNICO - EFECTIVIDAD EN LA ATENCIÓN DE LOS CANALES	El Proveedor debe garantizar tiempos de efectividad en la atención para cada canal como se detalla a continuación: • Línea telefónica nacional gratuita: <= 5 minutos. • Plataforma web para registro y monitoreo de tiquetes: <= 8 segundos. • Correo electrónico: <= 5 minutos. • Chat: <= 3 minutos.
SERVICIO DE SOPORTE TÉCNICO - NIVELES DE	El Proveedor debe Incluir el servicio de soporte técnico para el manejo de niveles 1 y 2 de soporte.

ATENCIÓN Y ESCALAMIENTO	Adicionalmente, el servicio de soporte técnico suministrado por el Proveedor debe gestionar escalamientos a nivel 3 o superior cuando corresponda. El proveedor del servicio de conectividad al inicio de la ejecución del contrato deberá entregar un documento en el que indique el nivel de escalamiento (Nombre del profesional, cargo, correo electrónico y número de celular de contacto) con al menos tres (3) profesionales asignados por el proveedor que permitan, elevar los requerimientos en caso de la no atención satisfactoria de las solicitudes. los perfiles asignados deberán ser al menos en el nivel 1. tecnólogo, y en los niveles 2 y 3 profesionales con vinculación con el proponente.
SERVICIO DE SOPORTE TÉCNICO - PRIORIZACIÓN DE TICKETS	Los tiquetes deben ser clasificados y atendidos según su nivel de criticidad. Los criterios para llevar a cabo dicha clasificación son los siguientes: **Prioridad 1:** Emergencia - Una Falla que afecta un proceso critico de la Entidad. **Prioridad 2:** Degradación en el servicio - Una Falla que afecta el desempeño o confiabilidad de un proceso de la Entidad. **Prioridad 3:** Inquietud o solicitud - Solicitudes de soporte menores o de información que no tienen impacto en los procesos de la Entidad. Incluye: Solicitudes de cambios, cambios en configuraciones, habilitación de VPN, resolución de inquietudes y entrega de información.
SERVICIO DE SOPORTE TÉCNICO - REPORTES DE GESTIÓN	El Proveedor debe entregar reportes mensuales de mesa de ayuda al supervisor del contrato, que permitan monitorear las siguientes variables: • Número de incidentes reportados según nivel de criticidad. • Número de incidentes resueltos que incluya el tiempo promedio de resolución según nivel de criticidad. • Análisis de causa raíz para incidentes relacionados. • Propuestas de mejora continua para los servicios contratados. • 2 variables más que defina la Entidad Compradora. La Entidad Compradora definirá las variables teniendo en cuenta que puedan ser soportados por la herramienta de monitoreo del Proveedor. El Proveedor debe entregar un reporte consolidado de mesa de ayuda una vez concluya el servicio de conectividad contratado. El proveedor debe contar con una plataforma que le permita al DANE visualizar consumo de canales en tiempo real y enviar reportes automáticos mensuales.
OBRA CIVIL	El Proveedor debe incluir la solución de última milla por el medio de transmisión adecuado para cumplir con los requerimientos del DANE. El servicio suministrado por el Proveedor incluye los costos y responsabilidades que significa adecuar la obra civil desde sus instalaciones (las del Proveedor) hasta cada uno de los puntos indicados donde se requiere el servicio. El Proveedor debe incluir la solución de última milla por el medio de transmisión adecuado para cumplir con los requerimientos de la Entidad Compradora y que están alineados con las condiciones y ANS definidos para el servicio. En caso de que se requiera y de ser necesario adelantar una obra civil, en las instalaciones de la Entidad o alguna de sus sedes, esta se entiende como:

	canalización con tubería EMT (Electrical Metallic Tubing), que corresponde al tendido de cables instalados a través de canalizaciones que contienen los ductos que permiten el tendido, la protección y el mantenimiento de cables de red y también de cables de fibra óptica. Se debe contemplar la instalación, adecuación y señalización de cables o fibra sobre canaletas de las instalaciones de la Entidad. El Proveedor debe estimar el costo total de la obra civil desde la acometida hasta el punto donde la Entidad requiere el enlace e incluirlo en el valor de instalación. Los costos en que incurra el Proveedor por la obra civil desde sus instalaciones (las del Proveedor) hasta la acometida en las sedes de la Entidad son responsabilidad del Proveedor.
TIEMPOS DE INSTALACIÓN	Es el tiempo máximo que puede tardar el Proveedor en hacer las instalaciones sin incurrir en incumplimiento, los cuales se solicitan de la siguiente manera: <= 50 días calendario
NOTIFICACIÓN DE INCIDENTES Y ENTREGA DE INFORMES DE INDISPONIBILIDAD	El proveedor del servicio deberá notificar los incidentes mediante al menos dos medios diferentes de comunicaciones (SMS, Correo electrónico, aplicaciones como WhatsApp, entre otros) que la Entidad determine y al personal que defina. Adicionalmente la Entidad, podrá establecer o delimitar el tipo de incidentes desea que le sean reportados de acuerdo con el nivel de criticidad. El proveedor del servicio tendrá 24 horas a partir del momento de un incidente crítico para reportarle a la Entidad Compradora el informe detallado. En el cual deberá relacionar al menos motivo de la falla, tiempo de indisponibilidad, elementos y servicios afectados, mecanismo utilizado en la solución del incidente crítico y mecanismos de prevención del incidente a futuro. El proveedor del servicio determinará el formato utilizado para el informe siempre y cuando se cuente con al menos la información solicitada.
RESPONSABILIDADES	El Proveedor administra la seguridad de la infraestructura y servicios de los elementos que tiene bajo su responsabilidad para la prestación de servicio. El Proveedor pondrá a disposición la tecnología necesaria para garantizar la seguridad de los servicios: autenticación, cifrado y controles de conexión a la red. Adicionalmente, El Proveedor suministrará los parámetros técnicos y procedimientos para garantizar la seguridad de los servicios.
QoS y CoS	El Proveedor debe brindar en los enlaces QoS (Calidad de Servicio) y CoS (Clase de Servicio) en los casos en que la Entidad Compradora lo requiera.
PROTOCOLO SNMP	El Proveedor debe garantizar que todos los equipos necesarios, tienen habilitado el protocolo SNMP para poder supervisar el funcionamiento de la red.
PUERTOS	Se solicita que el equipo CPE de cada enlace tenga al menos 4 puertos RJ45 utilizables.

3 PLANES DE DATOS PARA DISPOSITIVOS MÓVILES

GENERALIDADES	El propósito de este servicio es la conectividad mediante redes móviles 3G/4G con configuración de APN para brindar conectividad a los dispositivos móviles de captura (DMC) por medio de la adquisición de planes de datos para cada equipo, que permitan

<table>
<tr><td></td><td>realizar la transmisión de la información teniendo en cuenta las características técnicas requeridas por la Entidad. El oferente debe suministrar la conectividad necesaria para que el tráfico de este APN se entregue al Firewall de Nueva Generación ofertado de manera que la Entidad tenga control del acceso a contenidos.

Las Sim-Cards serán entregadas por el proveedor para verificación de características y alistamiento en la sede DANE CENTRAL ubicada en la Carrera 59 No. 26-70 Int 1- CAN de la ciudad de Bogotá D.C. y se suscribirá la respectiva acta de entrega a satisfacción por parte del supervisor del contrato.

El contratista debe ser un operador con red propia para la prestación del servicio de telefonía móvil celular.

El contratista debe ser un operador de telecomunicaciones móvil, no podrán ser representantes de marca o distribuidores autorizados.</td></tr>
<tr><td>CAPACIDAD DE DATOS</td><td>Plan de datos de mínimo 30GB</td></tr>
<tr><td>SIM CARD/PLANES DE DATOS</td><td>8986 unidades</td></tr>
<tr><td>TECNOLOGÍAS INALÁMBRICAS</td><td>4G, 3G</td></tr>
<tr><td>FECHA DE INICIO DEL SERVICIO</td><td>La fecha de inicio de estos servicios será de acuerdo con la solicitud del supervisor del contrato en la fecha que se indicará de acuerdo con la necesidad de la Entidad.</td></tr>
<tr><td>DURACIÓN</td><td>Se solicitan diferentes periodos para los planes de datos para satisfacer la necesidad institucional los cuales se presentan en la siguiente tabla:

<table>
<tr><th>OPERACIÓN</th><th>CANTIDAD</th><th>TIEMPO REQUERIDO</th></tr>
<tr><td>Recuento de unidades de observación</td><td>1518</td><td>3 meses</td></tr>
<tr><td>Operativo Censo Económico Barrido-Rutas</td><td>7464</td><td>4 meses</td></tr>
<tr><td>Otros Servicios</td><td>4</td><td>9 meses</td></tr>
<tr><td>Total</td><td>8986</td><td></td></tr>
</table></td></tr>
<tr><td>TIPOS DE TERMINALES</td><td>La entidad hará uso de los equipos terminales móviles que tenga dentro de su inventario de bienes (tabletas o dispositivos móviles de captura), para lo cual el proveedor entregará las SIM CARDS requeridas al supervisor del contrato o persona designada por este, las cuales deberán ser compatibles con los formatos SIM, mini SIM, micro SIM, nano SIM.

Exclusivamente para los cuatro (4) planes móviles requeridos para otros servicios, se requiere que el proveedor entregue con el servicio equipos terminales (MODEM WIFI PORTABLE). Estos dispositivos deben contar con la capacidad de conectar como mínimo 5 usuarios a través de cable y wifi, y deben ser compatibles con las diversas tecnologías proporcionadas por los proveedores del servicio.

El servicio incluye que estos terminales sean entregados por el proveedor a la Entidad en la modalidad de servicio.

Nota 1. No serán aceptados para entregar a la Entidad terminales USB para brindar el servicio de Internet móvil.

Nota 2. En el alcance de este servicio no está contemplado suministro de Smartphones.</td></tr>
</table>

<table>
<tr><td></td><td>Nota 3. El Proveedor entregará las SIM CARDS que cumplan con las características requeridas para la prestación del servicio. Las SIM CARDS no tendrán costos adicionales para la Entidad.</td></tr>
<tr><td>CONTROL DE CONTENIDOS</td><td>El servicio debe permitir la parametrización de categorías de contenidos y direcciones a las cuales podrán acceder los usuarios y bloquear los contenidos que por políticas de la entidad no requiere que sean descargados</td></tr>
<tr><td>COBERTURA REQUERIDA PARA LOS PLANES DE DATOS</td><td>El servicio se debe brindar con la mejor tecnología disponible en los municipios en los que el DANE requiere realizar sus operaciones censales.

• En zonas sin cobertura 4G LTE se debe garantizar la conexión a las redes 3G del Proveedor.

• El oferente debe contar con una herramienta publica donde se pueda validar la cobertura propuesta.

• El proveedor debe contar con registro TIC vigente y estar habilitado mínimo en las siguientes categorías: Telefonía móvil celular, proveedor de servicios de valor agregado y telemáticos, TPBC larga distancia.

Los municipios en los cuales se debe garantizar la cobertura de los planes de datos móviles son los siguientes:

<table>
<tr><th>ID</th><th>DEPARTAMENTO</th><th>MUNICIPIO</th></tr>
<tr><td>1</td><td>LA GUAJIRA</td><td>MAICAO</td></tr>
<tr><td>2</td><td>LA GUAJIRA</td><td>RIOHACHA</td></tr>
<tr><td>3</td><td>LA GUAJIRA</td><td>MANAURE</td></tr>
<tr><td>4</td><td>LA GUAJIRA</td><td>URIBIA</td></tr>
<tr><td>5</td><td>LA GUAJIRA</td><td>NAZARTEH (URIBIA)</td></tr>
<tr><td>6</td><td>AMAZONAS</td><td>LETICIA</td></tr>
<tr><td>7</td><td>ANTIOQUIA</td><td>MEDELLÍN</td></tr>
<tr><td>8</td><td>ANTIOQUIA</td><td>APARTADÓ</td></tr>
<tr><td>9</td><td>ANTIOQUIA</td><td>TURBO</td></tr>
<tr><td>10</td><td>ANTIOQUIA</td><td>CAUCASIA</td></tr>
<tr><td>11</td><td>ANTIOQUIA</td><td>SABANETA</td></tr>
<tr><td>12</td><td>ANTIOQUIA</td><td>ITAGUI</td></tr>
<tr><td>13</td><td>ANTIOQUIA</td><td>BELLO</td></tr>
<tr><td>14</td><td>ANTIOQUIA</td><td>RIONEGRO</td></tr>
<tr><td>15</td><td>ANTIOQUIA</td><td>CALDAS</td></tr>
<tr><td>16</td><td>ANTIOQUIA</td><td>ENVIGADO</td></tr>
<tr><td>17</td><td>ARAUCA</td><td>ARAUCA</td></tr>
<tr><td>18</td><td>ARAUCA</td><td>ARAUQUITA</td></tr>
<tr><td>19</td><td>ARAUCA</td><td>SARAVENA</td></tr>
<tr><td>20</td><td>ARAUCA</td><td>TAME</td></tr>
<tr><td>21</td><td>ATLANTICO</td><td>BARRANQUILLA</td></tr>
<tr><td>22</td><td>ATLANTICO</td><td>MALAMBO</td></tr>
<tr><td>23</td><td>ATLANTICO</td><td>SABANALARGA</td></tr>
</table>
</td></tr>
</table>

	24	ATLANTICO	SOLEDAD
	25	BOGOTA	BOGOTA
	26	BOLIVAR	CARTAGENA
	27	BOLIVAR	MAGANGUÉ
	28	BOLIVAR	TURBACO
	29	BOYACÁ	TUNJA
	30	BOYACÁ	CHIQUINQUIRA
	31	BOYACÁ	SOGAMOSO
	32	BOYACÁ	DUITAMA
	33	CALDAS	MANIZALES
	34	CALDAS	LA DORADA
	35	CAQUETA	FLORENCIA
	36	CASANARE	YOPAL
	37	CAUCA	POPAYÁN
	38	CAUCA	SANTANDER DE QUILICHAO
	39	CESAR	AGUACHICA
	40	CESAR	VALLEDUPAR
	41	CHOCO	QUIBDÓ
	42	CORDOBA	SAHAGUN
	43	CORDOBA	CERETÉ
	44	CORDOBA	LORICA
	45	CORDOBA	MONTERIA
	46	CORDOBA	PLANETA RICA
	47	CORDOBA	MONTELIBANO
	48	CUNDINAMARCA	ZIPAQUIRA
	49	CUNDINAMARCA	CAJICA
	50	CUNDINAMARCA	CHIA
	51	CUNDINAMARCA	FACATATIVÁ
	52	CUNDINAMARCA	MADRID
	53	CUNDINAMARCA	FUSAGASUGÁ
	54	CUNDINAMARCA	GIRARDOT
	55	CUNDINAMARCA	FUNZA
	56	CUNDINAMARCA	MOSQUERA
	57	CUNDINAMARCA	SOACHA
	58	GUAINIA	PUERTO INIRIDA
	59	GUAVIARE	SAN JOSÉ DEL GUAVIARE
	60	HUILA	NEIVA
	61	HUILA	GARZON
	62	HUILA	PITALITO
	63	MAGDALENA	CIÉNAGA

	64	MAGDALENA	EL BANCO
	65	MAGDALENA	SANTA MARTA
	66	META	VILLAVICENCIO
	67	META	ACACIAS
	68	META	GRANADA
	69	NARIÑO	IPIALES
	70	NARIÑO	PASTO
	71	NARIÑO	SAN ANDRÉS DE TUMACO
	72	NORTE DE SANTANDER	CÚCUTA
	73	NORTE DE SANTANDER	LOS PATIOS
	74	NORTE DE SANTANDER	OCAÑA
	75	NORTE DE SANTANDER	PAMPLONA
	76	NORTE DE SANTANDER	TIBÚ
	77	NORTE DE SANTANDER	VILLA DEL ROSARIO
	78	PUTUMAYO	MOCOA
	79	PUTUMAYO	PUERTO ASÍS
	80	QUINDIO	ARMENIA
	81	RISARALDA	PEREIRA
	82	RISARALDA	SANTA ROSA DE CABAL
	83	RISARALDA	DOSQUEBRADAS
	84	SAN ANDRES	SAN ANDRÉS
	85	SANTANDER	BARBOSA
	86	SANTANDER	BARRANCABERMEJA
	87	SANTANDER	BUCARAMANGA
	88	SANTANDER	FLORIDABLANCA
	89	SANTANDER	SAN GIL
	90	SANTANDER	GIRÓN
	91	SANTANDER	PIEDECUESTA
	92	SUCRE	SINCELEJO
	93	TOLIMA	ESPINAL
	94	TOLIMA	IBAGUE
	95	VALLE DEL CAUCA	BUENAVENTURA
	96	VALLE DEL CAUCA	CALI
	97	VALLE DEL CAUCA	CANDELARIA
	98	VALLE DEL CAUCA	CARTAGO
	99	VALLE DEL CAUCA	EL CERRITO
	100	VALLE DEL CAUCA	FLORIDA
	101	VALLE DEL CAUCA	GUADALAJARA DE BUGA
	102	VALLE DEL CAUCA	JAMUNDÍ
	103	VALLE DEL CAUCA	PALMIRA

	<table><tr><td>104</td><td>VALLE DEL CAUCA</td><td>PRADERA</td></tr><tr><td>105</td><td>VALLE DEL CAUCA</td><td>TULUÁ</td></tr><tr><td>106</td><td>VALLE DEL CAUCA</td><td>YUMBO</td></tr><tr><td>107</td><td>VAUPÉS</td><td>MITU</td></tr><tr><td>108</td><td>VICHADA</td><td>PUERTO CARREÑO</td></tr></table>
CONEXIÓN CON CENTRO DE DATOS DANE CENTRAL	El proveedor del servicio deberá configurar una red privada entre los dispositivos móviles que se encuentran haciendo uso del servicio móvil de datos incluido en las SIM CARDS entregadas y el Centro de Datos del DANE, el cual se encuentra ubicado en la ciudad de Bogotá D.C., en la Carrera 59 No. 26-70 interior 1 CAN, edificio DANE. El proveedor debe incluir todos los componentes tecnológicos para lograr tal fin. El proveedor debe garantizar la seguridad de la conexión con el firewall físico que se encuentra en el centro de datos de la Entidad mediante el cual se gestionaran los controles que se requieran para estos planes de datos.
CONEXIÓN NAP COLOMBIA E INTERNET	El servicio de Internet móvil debe incluir conexión al NAP Colombia
REPORTES	La Entidad podrá tener acceso a reportes del uso del servicio móvil de datos contratado, de acuerdo con las condiciones transversales del servicio (el proveedor debe monitorear el consumo de la capacidad de datos contratada y permitir la consulta diariamente).
SIM CARDS DE CONTINGENCIA	Se requiere que el proveedor reserve el 5% de las SIM CARD como contingencia en caso de pérdida o daño. En estos casos, se activará el plan de datos de la SIM CARD originalmente utilizada en la de contingencia de manera que se garantice la continuidad del servicio sin interrupciones debido a problemas con las SIM CARD.
DISPONIBILIDAD	La disponibilidad se mide usando la siguiente ecuación: $$\left(1 - \frac{Número\ total\ de\ minutos\ en\ que\ el\ servico\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ contratados\ x\ 24\ horas\ x\ 60\ minutos}\right) x\ 100\%$$ La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio de intercambio de datos sobre el enlace no está disponible, dividido en el número total de minutos en el mes facturado. La medición la hace el Proveedor monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Proveedor para que puedan ser consultados por la Entidad Compradora en cualquier momento durante la duración del servicio. La información mantenida por el Proveedor le debe permitir a la Entidad Compradora verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso. La medición se hace de forma individual sobre cada enlace. Es decir, cada enlace debe cumplir con el valor exigido en el ANS. **Disponibilidad exigida >=99.6% mensual** **Penalidad por no conformidad - Descuento en facturación** • 99%<=Disponibilidad<99.6%: 10% de descuento sobre el costo este servicio. • 98%<=Disponibilidad<99%: 20% de descuento sobre el costo este servicio. • 97%<=Disponibilidad<98%: 50% de descuento sobre el costo este servicio. • Disponibilidad<97%: 100% de descuento sobre el costo este servicio.

EFECTIVIDAD EN LA ENTREGA DEL SERVICIO	Mide el tiempo que tarda el Proveedor en hacer la entrega a la Entidad de las Sim Card activados para el uso del servicio de Internet móvil y penaliza las entregas que superan los tiempos definidos. Duración de la entrega del servicio según la cantidad de terminales y Sim Card. Más de 400 Sim Card <=20 días calendario **Penalidad por no conformidad - Descuento en facturación** • Duración de entrega del servicio máxima + 1 día calendario de retraso: 10% de descuento sobre el costo este servicio. • Duración de entrega del servicio máxima + 3 días calendario de retraso: 20% de descuento sobre el costo este servicio. • Duración de entrega del servicio máxima + 6 días calendario de retraso: 50% de descuento sobre el costo este servicio. • Duración de entrega del servicio máxima + >8 días calendario de retraso: 100% de descuento sobre el costo este servicio.
REGISTRO TIC	El Proveedor para la prestación de los servicios de telecomunicaciones solicitados, deberá contar con el Registro TIC emitido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones el cual lo acredita como Proveedor de Redes y Servicios de Telecomunicaciones en el territorio nacional. EL Registro TIC deberá estar vigente durante toda la ejecución del contrato.
SERVICIO DE SOPORTE TÉCNICO	El Proveedor debe tener la capacidad de brindar servicio de soporte técnico remoto para los servicios contratados por la Entidad. El Proveedor debe brindar soporte remoto para evaluar y solucionar Fallas e Interrupciones que se presenten en los servicios contratados por la Entidad Compradora. Adicionalmente, el Proveedor debe brindar soporte remoto a nivel nacional a través de los siguientes canales: - Línea de atención telefónica gratuita con cobertura nacional. - Plataforma web para registro y monitoreo de tiquetes. - Correo electrónico. - Chat. El Proveedor debe garantizar que cuenta con un servicio de mesa de ayuda el cual deberá operar en instalaciones a cargo del proveedor. El Proveedor debe garantizar que exista un tiquete por cada reporte de Falla o Interrupción que haga el DANE. Los canales de soporte deben estar disponibles 7x24 durante el tiempo de ejecución del contrato. El grupo de soporte del Proveedor debe garantizar que los tickets: • Sean registrados, clasificados y asignados según su criticidad. • Sean resueltos en los tiempos acordados en los ANS. • Tengan un seguimiento adecuado. • Cumplan con esquemas de escalamiento definidos.

	Deben ser documentados con las respectivas evidencias y en caso de requerir atención en sitio anexar registros fotográficos donde se observe Georreferenciación, fecha y hora donde ocurrió el evento.
SERVICIO DE SOPORTE TÉCNICO - PRIORIZACIÓN DE TICKETS	Los tiquetes deben ser clasificados y atendidos según su nivel de criticidad. Los criterios para llevar a cabo dicha clasificación son los siguientes: **Prioridad 1:** Emergencia - Una Falla que afecta un proceso critico de la Entidad. **Prioridad 2:** Degradación en el servicio - Una Falla que afecta el desempeño o confiabilidad de un proceso de la Entidad. **Prioridad 3:** Inquietud o solicitud - Solicitudes de soporte menores o de información que no tienen impacto en los procesos de la Entidad. Incluye: Solicitudes de cambios, cambios en configuraciones, habilitación de VPN, resolución de inquietudes y entrega de información.

4 ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIONES DE CONECTIVIDAD WIFI

ALCANCE	La Entidad requiere la adquisición, instalación y configuración de soluciones de conectividad para fortalecer la prestación de los servicios TIC de sedes y Centros Operativos Municipales en cumplimiento de la misionalidad de la Entidad. **NOTA: El alcance de ítem es la adquisición, implementación y garantía y soporte por 3 años de las plataformas descritas a continuación en las sedes del DANE y centros operativos municipales.**
CONDICIONES GENERALES DEL PROCESO	• Los elementos a adquirirse a nivel de hardware (appliances) y software, deben ser de propósito específico para WiFi. No se admiten componentes genéricos armados con sistemas operativos estándar sin preparación y aseguramiento del fabricante para el propósito específico de respaldo de datos. • Todos los componentes del sistema de WiFi, deberán ser de último modelo disponible por el fabricante en el momento de presentar la oferta y contar con todas las actualizaciones que este disponga, durante el periodo de garantía y soporte adquiridos. • Evidenciar mediante documento emitido por el fabricante, que todos los bienes que hacen parte del sistema de seguridad perimetral ofertado sean nuevos, no aparezcan en listas end-of-life o end-of-sale ó end-of-support del fabricante y cuentan con soporte para los próximos cinco (5) años • Todos los equipos y su plataforma de administración y gestión a adquirirse deberán ser trasladadas, montadas, instaladas, configuradas, parametrizadas, probadas y puestas en marcha en el DANE central, sedes territoriales y Centros operativos municipales (COM) • El soporte técnico a todos los equipos y sus plataformas de administración y gestión a adquirirse, al igual que la garantía será por un periodo de tres (3) años y en modalidad 7x24x4 (siete días a la semana, veinticuatro horas al día, con un tiempo de respuesta de cuatro horas)

<table>
<tr><td></td><td>

- Con la propuesta el oferente debe entregar las URL y Datasheets públicos elaborados por el fabricante, que sustenten el cumplimiento de los requerimientos técnicos exigidos, indicando el número de folio o página del datasheet o URL que demuestre que cumple con cada uno de los ítems requeridos para el presente proceso. No se aceptarán cartas, documentos armados por el proponente o certificaciones firmadas por personal de los fabricantes participantes que avalan el cumplimiento de estos requerimientos.
- Instalación, configuración, parametrización, pruebas de funcionamiento, puesta en marcha, soporte y garantía del sistema de WiFi.
- La implementación de todos los sistemas de WiFi, están compuestos por todos sus componentes a nivel de hardware, software y accesorios a nivel eléctrico (cables de conexión, acometidas y accesorios no descritos en este estudio, pero que hagan parte de la instalación), ambiental (tornillos, rieles y demás elementos físicos que hagan parte de la instalación del appliance), y desplazamientos de equipos al interior de la ciudad de Bogotá y el resto de sedes del DANE a nivel nacional, serán suministrado por el proponente.
- El proponente debe adjuntar carta del fabricante, donde certifique que es distribuidor autorizado para Colombia de los productos o servicios ofertados como Partner en el nivel más alto membresía del Fabricante. La certificación no debe superar una antigüedad mayor de treinta (30) días anteriores a la fecha del cierre del presente proceso.
- El proponente debe adjuntar carta del fabricante dirigida a la entidad con el número del proceso, donde certifique que es distribuidor autorizado para Colombia de los productos o servicios ofertados con la especialización de SD-WAN. Esto para garantizar que se integre a las soluciones ofertadas de conectividad de las sedes del DANE y las sedes de los Centros Operativos Municipales COM. La certificación no debe superar una antigüedad mayor de treinta (30) días anteriores a la fecha del cierre del presente proceso.
-

El oferente debe suministrar e implementar los siguientes elementos para la entidad:

</td></tr>
<tr><td>CANTIDADES REQUERIDAS</td><td>

- Access Point Indoor: 300
- Controladoras de WIFI y Seguridad: 2

</td></tr>
<tr><td>UBICACIÓN DE LA SOLUCIÓN</td><td>

- El proponente se encargará de la instalación y configuración de los Access Point en las sedes territoriales del DANE y los Centros Operativos Municipales (COM), destinados para la implementación de los canales de datos, de acuerdo con las especificaciones detalladas en la presente ficha técnica.

  Asimismo, llevará a cabo la instalación y configuración de los equipos de la controladora de WiFi y seguridad en el centro de datos de la Entidad, ubicado en la ciudad de Bogotá, conforme a las especificaciones técnicas establecidas en la presente ficha técnica.

- El proponente deberá configurar los puntos de acceso en las respectivas sedes a nivel nacional que se conectaran a las redes MPLS para lograr integración con la Controladora WIFI y de seguridad que se encontrará en el datacenter de la sede Central del DANE en la ciudad de Bogotá.

</td></tr>
<tr><td>TIEMPO DE ENTREGA</td><td>

La solución de red inalámbrica con todos sus componentes deberá ser implementada y funcional en un plazo de **50 días calendario** en las sedes a nivel nacional de acuerdo con la siguiente distribución:

<table>
<tr><th colspan="4">SEDES DANE</th></tr>
<tr><th>ID</th><th>Sede</th><th>Dirección</th><th>Cantidad APS a instalar</th></tr>
</table>

</td></tr>
</table>

1	BOGOTA - DANE CENTRAL	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	32
2	BOGOTA - DANE CENTRAL	Carrera 59 # 26 - 70 CAN Interior 1 Edificio DANE - Bogotá	
3	BOGOTA - CASA ESMERALDA	Cr 59A No 44A-30 Bogotá	2
4	BOGOTA - ALAMOS	Calle 64G No. 92 - 56 / Álamos Industrial	8
5	TUNJA	Carrera 11 No. 20-41 Piso 4	2
6	NEIVA	Calle 18 No. 7-75 Barrio Quirinal	2
7	VILLAVICENCIO	Carrera 43D No. 16-06 Barrio El Buque	3
8	FLORENCIA	Calle 24 No. 4A - 49, Barrio la Libertad	2
9	YOPAL	Transversal 18 No. 7-05 Piso 4 Centro	2
10	BARRANQUILLA	Calle 72 No. 58 - 65 Piso 1 y 2, ED. CENTRO	5
11	CARTAGENA	Bosque Sector San Isidro, Transversal 54 No. 28 – 25 Edificio Movisol 4 piso	2
12	SINCELEJO	Calle 25 No. 24-64 Piso 3	2
13	SANTA MARTA	Calle 17A No. 9-104 Barrio el pueblito	2
14	RIOHACHA	Carrera 11 No. 13 -39 Barrio Libertador	2
15	VALLEDUPAR	Carrera 6 No. 15-32 Plaza Alfonso López	2
16	SAN ANDRES	Avenida Francisco Newball No. 9- 184 Sector Los Almendros	3

17	CUCUTA	Calle 13 No. 5 - 09 Centro Primer Piso	5
18	BUCARAMANGA	Calle 22 No 24 - 54 Barrio Alarcón	4
19	ARAUCA	Calle 21 No.15 - 13 Barrio Santa Teresita	2
20	CALI	Avenida 6B Norte No. 26N – 55 Barrio Santa Mónica Residencial	5
21	PASTO	Calle 20A No. 28-19 piso 2 al 5	5
22	POPAYAN	Carrera 9 No. 8N-20 Barrio Belalcázar	4
23	MANIZALES	Calle 77 No. 21-69 Barrio Milán	3
24	ARMENIA	CALLE 20 A No. 15-16 Edificio Torre Yanuba Piso 3	3
25	PEREIRA	Calle 19 No. 9-75, Edificio Palacio Nacional. Piso 3	3
26	MEDELLIN	Calle 44 No. 65 - 23 Barrio San Joaquín	4
27	MONTERIA	Calle 32 No. 10-44 Centro La Ceiba	2
28	QUIBDO	Carrera 9 No. 25-68 Barrio Alameda Reyes Edificio Cínica Citará Oral	3
29	IBAGUE	Calle 11 No. 3-32 Edificio Banco de la República Piso 7	2
30	BOGOTA, CORABASTOS	Avenida Carrera 80 No. 2 54, CORABASTOS, BODEGA 47 LOCAL 0501	1
31	SAN JOSE DEL GUAVIARE	Calle 5A No. 27 - 16, barrio 20 de Julio	2
TOTAL			**119**

SEDES DANE			
ID	**Sede**	**Dirección**	**Cantidad APS a instalar**
1	MITU		2

		CARRERA 14 N° 12 - 43 LOCAL 3 HOTEL JM	
2	PUERTO CARREÑO	CARRERA 11 NO. 19- 81/93 BARRIO LAS ACACIAS	2
3	LETICIA	Carrera 7 No. 6-104 Barrio Punto Brava	5
4	PUERTO INIRIDA	Calle 17 No. 13-36 Barrio los Libertadores	2
TOTAL			**11**

SEDES CENSO ECONOMICO			
ID	**DEPARTAMENTO**	**MUNICIPIO**	**Cantidad APS a instalar**
1	BOGOTA	BOGOTA	10
2	CALDAS	MANIZALES 1	1
3	TOLIMA	ESPINAL	1
4	RISARALDA	PEREIRA	3
5	TOLIMA	IBAGUE 1	1
6	RISARALDA	SANTA ROSA DE CABAL	1
7	RISARALDA	DOSQUEBRADAS	1
8	QUINDIO	ARMENIA 1	1
9	QUINDIO	ARMENIA 2	1
10	CALDAS	MANIZALES 2	1
11	CALDAS	LA DORADA	1
12	TOLIMA	IBAGUE 2	1
13	TOLIMA	IBAGUE 3	1
14	TOLIMA	IBAGUE 4	1
15	CAQUETA	FLORENCIA	2
16	HUILA	NEIVA	3
17	GUAVIARE	SAN JOSÉ DEL GUAVIARE	1
18	META	VILLAVICENCIO	4
19	CASANARE	YOPAL	2
20	AMAZONAS	LETICIA	1
21	META	ACACIAS	1
22	META	GRANADA	1
23	BOYACÁ	TUNJA	2
24	BOYACÁ	CHIQUINQUIRA	1
25	BOYACÁ	SOGAMOSO	1
26	BOYACÁ	DUITAMA	1
27	HUILA	GARZON	1
28	HUILA	PITALITO	1

29	CUNDINAMARCA	ZIPAQUIRA	1
30	CUNDINAMARCA	CAJICA	1
31	CUNDINAMARCA	CHIA	1
32	CUNDINAMARCA	FACATATIVÁ	1
33	CUNDINAMARCA	MADRID	1
34	CUNDINAMARCA	FUSAGASUGÁ	1
35	CUNDINAMARCA	GIRARDOT	1
36	CUNDINAMARCA	FUNZA	1
37	CUNDINAMARCA	MOSQUERA	1
38	CUNDINAMARCA	SOACHA	2
39	CORDOBA	SAHAGUN	1
40	CORDOBA	CERETÉ	1
41	CORDOBA	LORICA	1
42	CORDOBA	MONTERIA	3
43	CORDOBA	PLANETA RICA	1
44	CORDOBA	MONTELIBANO	1
45	ANTIOQUIA	MEDELLÍN 1	2
46	ANTIOQUIA	MEDELLÍN 2	2
47	ANTIOQUIA	MEDELLÍN 3	2
48	ANTIOQUIA	MEDELLÍN 4	2
49	ANTIOQUIA	APARTADÓ	1
50	ANTIOQUIA	TURBO	1
51	ANTIOQUIA	CAUCASIA	1
52	ANTIOQUIA	SABANETA	1
53	ANTIOQUIA	ITAGUI	2
54	ANTIOQUIA	BELLO	1
55	ANTIOQUIA	RIONEGRO	1
56	ANTIOQUIA	CALDAS	1
57	ANTIOQUIA	ENVIGADO	1
58	CHOCO	QUIBDÓ	1
59	ARAUCA	ARAUCA	1
60	ARAUCA	ARAUQUITA	1
61	ARAUCA	SARAVENA	1
62	SANTANDER	BARBOSA	1
63	SANTANDER	BARRANCABERMEJA	2
64	SANTANDER	BUCARAMANGA	4
65	SANTANDER	FLORIDABLANCA	2
66	SANTANDER	SAN GIL	1
67	NORTE DE SANTANDER	CÚCUTA	4
68	NORTE DE SANTANDER	LOS PATIOS	1

69	NORTE DE SANTANDER	OCAÑA	1
70	NORTE DE SANTANDER	PAMPLONA	1
71	NORTE DE SANTANDER	TIBÚ	1
72	NORTE DE SANTANDER	VILLA DEL ROSARIO	1
73	ARAUCA	TAME	1
74	SANTANDER	GIRÓN	1
75	SANTANDER	PIEDECUESTA	1
76	VALLE DEL CAUCA	BUENAVENTURA	1
77	VALLE DEL CAUCA	CALI 1	2
78	VALLE DEL CAUCA	CALI 2	2
79	VALLE DEL CAUCA	CALI 3	2
80	VALLE DEL CAUCA	CALI 4	2
81	VALLE DEL CAUCA	CANDELARIA	1
82	VALLE DEL CAUCA	CARTAGO	1
83	VALLE DEL CAUCA	EL CERRITO	1
84	VALLE DEL CAUCA	FLORIDA	1
85	VALLE DEL CAUCA	GUADALAJARA DE BUGA	1
86	VALLE DEL CAUCA	JAMUNDÍ	1
87	VALLE DEL CAUCA	PALMIRA	1
88	VALLE DEL CAUCA	PRADERA	1
89	VALLE DEL CAUCA	TULUÁ	2
90	VALLE DEL CAUCA	YUMBO	1
91	PUTUMAYO	MOCOA	1
92	PUTUMAYO	PUERTO ASÍS	1
93	NARIÑO	IPIALES	1
94	NARIÑO	PASTO	3
95	NARIÑO	SAN ANDRÉS DE TUMACO	1
96	CAUCA	POPAYÁN	2
97	CAUCA	SANTANDER DE QUILICHAO	1
98	ATLANTICO	BARRANQUILLA	4
99	ATLANTICO	MALAMBO	1
100	ATLANTICO	SABANALARGA	1
101	ATLANTICO	SOLEDAD	3
102	BOLIVAR	CARTAGENA	4
103	BOLIVAR	MAGANGUÉ	1
104	BOLIVAR	TURBACO	1
105	GUAJIRA	MAICAO	1
106	GUAJIRA	RIOHACHA	2
107	SAN ANDRES	SAN ANDRÉS	1
108	MAGDALENA	CIÉNAGA	1

	<table><tr><td>109</td><td>MAGDALENA</td><td>EL BANCO</td><td>1</td></tr><tr><td>110</td><td>MAGDALENA</td><td>SANTA MARTA</td><td>3</td></tr><tr><td>111</td><td>SUCRE</td><td>SINCELEJO</td><td>2</td></tr><tr><td>112</td><td>CESAR</td><td>AGUACHICA</td><td>1</td></tr><tr><td>113</td><td>CESAR</td><td>VALLEDUPAR</td><td>3</td></tr><tr><td colspan="3">TOTAL</td><td>170</td></tr></table>
CARACTERÍSTICAS GENERALES DE LA SOLUCIÓN DE RED INALAMBRICA	• Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia. • Todos los equipos de punto de acceso inalámbrico deberán ser administrados de forma centralizada a través de la controladora inalámbrica ofertada en Onpremise. No se aceptan soluciones de controladora en nube. • Debe permitir administrarse remotamente a través de enlaces WAN. • El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico. • Los puntos de acceso implementados deben ser monomarca, nuevos y deberán ser compatibles y permitir integración nativa con el firewall (cumpliendo funciones de controladora de WiFi) de nueva generación solicitado para este proceso. • Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC; la entidad entregara los túneles entre la sede principal y la sedes remotas. • Debe permitir, en caso de ser necesario, el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (conmutación local), es decir, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico. • Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica. • En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. • Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora. • Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs. • En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS/wIPS). • En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red; • En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES). • En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;

	• Debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP. • Debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming. • Debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming. • Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos. • Debe implementar el estándar IEEE 802.11e. • Debe implementar el estándar IEEE 802.11h. • El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU. • El punto de acceso deberá soportar (LPDC) - Low Density Parity Check. • El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation. • El Punto de Acceso deberá soportar metodo de diversidad (MRC) Maximum Ratio Combining. • Debe tener indicadores luminosos (LED) para indicación de estado. • Debe permitir su alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3af, 802.3at o 802.3bt. • Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada. • La solución de red inalámbrica debe permitir la implementación de un portal cautivo sin necesidad de equipos o software adicional. Este portal puede desplegarse por SSID. • La solución de red inalámbrica ofertada debe integrarse nativa a la plataforma de reportes de seguridad con la que cuenta la entidad, permitiendo la generación de reportes centralizados y recolección de logs desde esta plataforma centralizada. • La solución de red inalámbrica debe soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos. • La solución de red inalámbrica debe soportar IPv4 e IPv6 por SSID. • La solución de red inalámbrica debe soportar monitoreo y supresión de puntos de acceso indebidos. • Uno de los radios de cada Access Point debe poderse configurar como monitor del espectro en búsqueda de access points intrusos. • La solución de red inalámbrica debe proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS.
CARACTERÍSTICAS DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Las controladoras deben estar implementadas en alta disponibilidad. • Las controladoras deben permitir la segmentación e independización de los APs y administración de los Access points de las sedes nacionales del DANE y los Access points de las sedes del Censo Económico, mediante la separación en controladoras independientes virtuales dentro de la misma controladora física. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por usuario. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por IP. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por canal.

	• La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal. • La solución de red inalámbrica debe permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación. • La solución de red inalámbrica debe soportar Fast Roaming en autenticación con portal cautivo. • La solución de red inalámbrica debe permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico. • La solución de red inalámbrica debe ser compatible con el protocolo 802.1x RADIUS. • La controladora debe permitir métodos de descubrimiento de puntos de acceso de manera automática. • La controladora debe permitir métodos de descubrimiento de puntos de acceso por IP estática. • La controladora debe permitir métodos de descubrimiento de puntos de acceso por DHCP. • La controladora debe permitir métodos de descubrimiento de puntos de acceso por DNS. • La controladora debe permitir métodos de descubrimiento de puntos de acceso por Broadcast. • La controladora debe permitir métodos de descubrimiento de puntos de acceso por Multicast. • La controladora inalámbrica debe suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue). • La controladora debe contar con protección contra ataques ARP Poisoning en el controlador inalámbrico. • La controladora debe contar con mecanismos de protección de tramas de administración de acuerdo con las especificaciones de la alianza Wi-Fi y estándar 802.11ac. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection. • La controladora inalámbrica debe tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge.

	• Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas. • La solución de red inalámbrica debe permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso. • La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible. • La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario. • La solución de red inalámbrica debe permitir configurar el número máximo de clientes que pueden ser permitidos por SSID. • La solución de red inalámbrica debe permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso. • La solución de red inalámbrica debe permitir configurar el número máximo de clientes que pueden ser permitidos por Radio. • La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh. • La solución de red inalámbrica debe ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico a los usuarios, con ajuste de tiempo de expiración de la contraseña. • La solución de red inalámbrica debe proporcionar un mecanismo de balanceo de tráfico/usuarios entre frecuencias y/o radios de los Puntos de Acceso. • La solución de red inalámbrica debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica. • La solución de red inalámbrica debe permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados. • La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz. • Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados. • Debe permitir asociaciones dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS. • Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling. • La solución de red inalámbrica debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza. • La controladora inalámbrica debe soportar una licencia que permita al menos 5000 firmas de aplicaciones para reconocimiento de tráfico. • La controladora inalámbrica debe tener interface de administración integrada en el mismo equipo. • El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales. • La controladora inalámbrica debe soportar protocolo LLDP. • Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos. • La solución de red inalámbrica debe soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire.

	• Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos. • La solución debe estar en capacidad de operar en modos de radio Background y dedicado para WIPS / WIDS. • La solución debe permitir el control de aplicaciones y uso de ancho de banda. • La solución debe contar con el aprovisionamiento automático de recursos de radio para optimización de rendimiento.
CARACTERÍSTICAS GENERALES DE FIREWALL DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), funcionando en alta disponibilidad (2 equipos de la misma referencia y características. • Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. • La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7. • Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación. • La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. • Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q. • Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP. • Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding para IPv4 e IPv6. • Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM). • Los dispositivos de protección de red deben soportar DHCP Relay. • Los dispositivos de protección de red deben soportar DHCP Server. • Los dispositivos de protección de red deben soportar sFlow. • Los dispositivos de protección de red deben soportar Jumbo Frames. • Debe permitir configuración de NAT dinámica (varios-a-1), NAT dinámica (muchos-a-muchos), NAT estática (1-a-1) , NAT estática (muchos-a-muchos), NAT estático bidireccional 1-a-1, traducción de puertos (PAT). • Debe soportar NAT Origen, NAT destino, NAT de origen y NAT de destino de forma simultánea. • Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Debe ser compatible con NAT64 y NAT46. • Debe implementar el protocolo ECMP. • Debe soportar SD-WAN de forma nativa. • Debe soportar el balanceo de enlace hash por IP de origen. • Debe soportar el balanceo de enlace por hash de IP de origen y destino. • Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces. • Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red. • Enviar logs a sistemas de gestión externos simultáneamente. • Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Debe soporta protección contra la suplantación de identidad (anti-spoofing). • Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2, ISIS y BGP).

	• Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3, ISIS, BGP). • Soportar OSPF graceful restart. • Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Debe soportar la creación de sistemas virtuales en el mismo equipo, soportando al menos 10 sistemas virtuales incluidos completamente licenciados. • Para una alta disponibilidad, debe ser posible hacer distribución de la carga entre los diferentes contextos o firewall virtuales del equipo. • Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. • La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso. • Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos). • La consola de administración debe soportar como mínimo, inglés, español y portugués. • La consola debe soportar la administración de puntos de acceso para mejorar el nivel de seguridad. • La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
CARACTERÍSTICAS DE FIREWALL PERIMETRAL DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Debe soportar controles de zona de seguridad; • Debe contar con políticas de control por puerto y protocolo; • Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones; • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad; • Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;

	• Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall; • Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. • Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF); • Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes • En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN; • La solución debe soportar la integración nativa con la plataforma de sandboxing, protección de correo electrónico y Web application firewall de la entidad
CARACTERÍSTICAS DE CONTROL DE APLICACIONES DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. • Detección de miles de aplicaciones en 16 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico. • Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs. • Debe identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor. • Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante. • Actualización de la base de firmas de la aplicación de forma automática. • Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos. • Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas. • Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante. • Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; • Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc). • Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación.

CARACTERÍSTICAS DE PROTECCIÓN DE AMENAZAS DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo. • Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware). • Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante. • Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad. • Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos. • Deber permitir el bloqueo de vulnerabilidades y exploits conocidos. • Debe incluir la protección contra ataques de denegación de servicio. • Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo. • Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo. • Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP. • Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP. • Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets). • Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc. • Detectar y bloquear los escaneos de puertos de origen. • Bloquear ataques realizados por gusanos (worms) conocidos. • Contar con firmas específicas para la mitigación de ataques DoS y DDoS. • Contar con firmas para bloquear ataques de desbordamiento de memoria (buffer overflow). • Debe poder crear firmas personalizadas en la interfaz gráfica del producto; • Identificar y bloquear la comunicación con redes de bots. • Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo. • Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación. • Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos. • Los eventos deben identificar el país que origino la amenaza. • Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). • Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP. • Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad. • En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles.

	• Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).
CARACTERÍSTICAS DE PROTECCIÓN DE FILTRADO WEB DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora). • Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito. • Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL. • Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL. • Tener por lo menos 75 categorías de URL. • Debe tener la funcionalidad de exclusión de URLs por categoría. • Permitir página de bloqueo personalizada. • Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio). • Además del Explicit Web Proxy, soportar proxy web transparente.
CARACTERÍSTICAS DE MANEJO DE IDENTIDAD DE USUARIOS DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc. • Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios. • Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios. • Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo). • Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios. • Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD. • Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma; • Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores.

CARACTERÍSTICAS DE DATA LOSS PREVENTION DLP DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Permite la creación de filtros para archivos y datos predefinidos. • Los archivos deben ser identificados por tamaño y tipo. • Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones. • Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos. • Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos. • Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.GG
CARACTERÍSTICAS DE GEOLOCALIZACIÓN DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países. • Debe permitir la visualización de los países de origen y destino en los registros de acceso. • Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.
CARACTERÍSTICAS DE VPN DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Soporte VPN de sitio-a-sitio y cliente-a-sitio. • Soportar VPN IPSec. • Soportar VPN SSL. • La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512 • La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2). • La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. • Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting. • Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy. • Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL. • Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
CARACTERÍSTICAS DE DESEMPEÑO DE LAS CONTROLADORAS DE WIFI Y SEGURIDAD	• Desempeño de Firewall: 180 Gbps • Sesiones concurrentes: 7’000.000 • Nuevas conexiones por segundo: 600000 • Desempeño de VPN IPsec: 50 Gbps • Desempeño de VPN SSL: 5 Gbps • Usuarios concurrentes de VPN SSL: 10000 • Desempeño de IPS con tráfico empresarial: 18 Gbps • Desempeño de inspección SSL: 10 Gbps • Desempeño de Control de Aplicaciones: 40 Gbps

	• Desempeño de Firewall de Nueva Generación: 14 Gbps • Desempeño de Protección de Amenazas: 12 Gbps • Capacidad de administración de 1500 Access Points • Interfaces de 1 / 2.5 / 5 / 10 Gbps RJ45: 8 • Interfaces de administración: 2 de 1 Gbsp RJ-45 • Interfaces de 10 Gbps SFP+: 16 • Interfaces de 25 Gbps SFP: 8 • Interfaces de 100 / 40 Gbps: 2 • Almacenamiento: 480 GB
CARACTERÍSTICAS MÍNIMAS DE ACCESS POINTS INDOOR	• Cantidad de radios: 4 (incluyendo un radio BLE) • Cantidad de antenas: 8 internas • Ganancia de Antenas: 4 dBi para 2.4 GHz, 5.4 dBi para 5 GHz, 5.5 para 6 GHz • Modulación: QPSK, 64/256/1024 QAM • MIMO: 4x4, soporte de Multiuser MIMO UL DL • Tasa de datos: 8 Gbps • Interfaces: 2 multigigabit de 1 / 2.5 / 5 Gbps • Certificación: WiFi Alliance • Capacidad de usuarios por radio: 256 • Estándares Wifi: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax WiFi 6E

SERVICIOS PROFESIONALES Y GARANTÍA	• El contratista deberá realizar, a través de personal técnico certificado por el fabricante de la solución, la implementación, configuración y puesta en funcionamiento de la plataforma. Deberá cumplir mínimo con las siguientes tareas.
	  ○ Levantamiento de información previo a la instalación de la plataforma ofertada. Se debe realizar la instalación, configuración, parametrización, actualización, pruebas de funcionamiento y puesta en marcha de la solución.
	  ○ El contratista deberá realizar y ejecutar un protocolo de pruebas para la entrega a satisfacción de la solución, el cual será aprobado por el Supervisor del contrato. Se deben realizar las respectivas pruebas de funcionalidad y operatividad de todos y cada uno de los elementos, con el propósito de comprobar la calidad y cumplimiento de los requerimientos solicitados.
	• Se deberá suministrar soporte directo con fábrica durante un periodo de tres (3) años en la modalidad 7X24x4 (siete días a la semana, veinticuatro horas al día, con un tiempo de respuesta de cuatro horas) para la solución ofertada a la entidad y que se opere de forma unificada desde una única consola de gestión.
	• El soporte deberá incluir actualizaciones de firmware, acceso al portal de soporte del fabricante y recursos técnicos y base de conocimiento.
	• El contratista deberá atender y resolver cualquier problema técnico de la solución, en diferentes tipos de acceso (telefónico, e-mail, acceso remoto o presencial en caso de que así se requiera), este soporte deberá ser suministrado por personal especializado en la herramienta ofertada.
	• El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil. Para ello debe contar con un centro de servicio que cumpla con mínimo:
	  ○ Software de Mesa de Servicio, donde se puedan registrar casos o incidentes de forma web, correo o teléfono.
	  ○ Este software de mesa de ayuda debe cumplir con el marco de referencia ITIL
	  ○ Nivel de soporte 1 para atención remota, 2 para atención en sitio y 3 para soporte de especialista y escalamiento a fábrica.

	• Al finalizar cada visita correctiva y el contratista generará un informe de servicio con las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración. • El oferente deberá estar certificado en la norma ISO 27001 con el fin de garantizar que cumpla con todos los procesos de seguridad de la información que serán gestionados durante la prestación del servicio. El contratista debe presentar copia de la certificación ISO 27001 la cual deberá contener información del ente certificador para verificar la vigencia y autenticidad de esta. • El oferente contará con un SOC, el cual deberá ser miembro de First desde donde se monitoreará la controladora Wi-Fi desde el SIEM con el que cuenta la entidad. • El oferente deberá estar certificado en la norma ISO 9001 con el fin de garantizar que cumpla con todos los procesos de calidad que serán gestionados durante la prestación del servicio. El contratista debe presentar copia de la certificación ISO 9001 la cual deberá contener información del ente certificador para verificar la vigencia y autenticidad de esta. • El oferente deberá estar certificado en la norma ISO 20001 con el fin de garantizar que cumpla con todos los procesos para la prestación de servicio TI. El contratista debe presentar copia de la certificación ISO 20001 la cual deberá contener información del ente certificador para verificar la vigencia y autenticidad de esta.