DENOMINACIÓN DE BIEN O SERVICIO
SOLUCIÓN INTEGRAL DE SERVICIO DE INTERNET Y SEGURIDAD PERIMETRAL PARA LA POLICÍA NACIONAL.
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
SOLUCIÓN INTEGRAL DE SERVICIO DE INTERNET Y SEGURIDAD PERIMETRAL PARA LA POLICÍA NACIONAL.
UNIDAD DE MEDIDA
UNIDAD
DESCRIPCIÓN GENERAL
81112100 – 83121700 – 81111800 – 43223100

ÍTEM	SOLUCIÓN INTEGRAL DE SERVICIO DE INTERNET Y SEGURIDAD PERIMETRAL PARA LA POLICÍA NACIONAL
1.	**CARRIER DE INTERNET**
1.1.	Enlaces dedicados y conectividad a Internet (misión crítica). El último kilómetro será una solución implementada en fibra óptica redundante, que comunicará a la Policía Nacional con el Centro de Operaciones del ISP (entidad prestadora de servicio de internet).

LUGAR	UBICACIÓN	ANCHO DE BANDA	ÚLTIMA MILLA
Policía Nacional	Dirección General Carrera 59 No. 26-11 CAN Edificio OFTIC Bogotá Colombia	10 GBPS	Fibra Óptica
Datacenter Contingencia Policía Nacional	Carrera 106 No 15A - 25 Manzana 5 Lote 16A Zona Franca	1 GBPS	Fibra Óptica

El enlace de 1 GBPS será instalado en el Datacenter Contingencia de la Policía Nacional, ubicado en la Carrera 106 No 15A - 25 Manzana 5 Lote 16A Zona Franca, el cual se encuentra actualmente en funcionamiento a través del contrato de prestación de servicios PN-DIRAF No. 06-7-10229-23, el colocation y cross conexión del canal debe ser realizado por el contratista sin generar costo adicional a la Institución.
En caso de traslado del Datacenter Principal o de Contingencia de la Policía Nacional, el nuevo colocation y cross conexión del canal debe ser realizado por el contratista sin generar costo adicional a la Institución, garantizando el cumplimiento de la norma técnica aplicable y minimizando al máximo el periodo de indisponibilidad.

En consecuencia, el contratista garantizará:

a) Proveer un enlace dedicado (sin reúso garantizado) con capacidad mínima de 10 GBPS en la sede principal (Dirección General – CAN, Bogotá), con escalabilidad no disruptiva a mayores anchos de banda (sin cambio de última milla ni de puertos de acceso).
b) Proveer un enlace dedicado para contingencia/DR en el Datacenter de contingencia, con capacidad mínima de 1 GB, sin recambio físico.
c) Última milla 100% en fibra óptica con redundancia física real (rutas, ductos y nodos diferentes), demostrable mediante documentación técnica.
d) Entrega del servicio mediante interfaces Ethernet de capacidad suficiente para el canal contratado y su crecimiento futuro (mínimo 12G, preferible 25G/40G), evitando cuellos de botella.
e) Enrutamiento BGP para IPv4 e IPv6 (dual-stack), con alta disponibilidad y failover automático.
f) Conectividad nacional (NAP/IXP) e internacional con redundancia de salidas (mínimo dos rutas internacionales) sin dependencia de un único punto de falla.
g) El contratista suministrará y configurará dos (02) routers de borde (CPE) en alta disponibilidad (activo/activo o activo/pasivo), completamente independientes, instalados en el centro de datos de la Policía Nacional, sin costo adicional, incluyendo licencias, soporte y actualizaciones durante la vigencia del contrato.
h) Colocation y cross-conexión requeridas para la operación (incluyendo datacenter principal, de contingencia y eventuales traslados) estarán a cargo del contratista sin costo adicional para la Institución, con continuidad del servicio garantizada.

1.2.	**Periodo de transición**: El CONTRATISTA en el marco de la ejecución del contrato y con presupuesto de este, deberá: • Proveer la continuidad del servicio al momento de adjudicación del presente proceso, hasta tanto se instale la totalidad del nuevo servicio requerido en el apartado "*ESPECIFICACIONES TÉCNICAS MÍNIMAS*" y "*LUGARES Y CANTIDADES PRESTACIÓN SERVICIO*". • Proveer el servicio de instalación y puesta en funcionamiento de WLAN establecido en el anexo *"LUGARES Y CANTIDADES PRESTACIÓN SERVICIO"*. • Realizar la transición e instalación de la nueva solución en un tiempo no mayor a dos (02) meses, contados a partir de la firma del contrato. • El contratista entrante deberá garantizar el servicio de transmisión y obligaciones contempladas en el contrato de prestación de servicios PN DIRAF No. 06-7-10229-23, durante el periodo de transición a partir de la firma del contrato, por lo cual durante el tiempo que demore la instalación total y para no interrumpir el servicio, el contratista deberá asumir los gastos que se generen para sostener la operación por parte del antiguo contratista.
1.3.	Para la Policía Nacional: el único punto de conexión se ubicará en el rack indicado por esta entidad dentro del centro de datos de la misma. En este rack se ubican los siguientes elementos: • Una (01) bandeja de fibra de 19 pulgadas rackeable, que recibe la última milla en fibra óptica proveniente del proveedor de servicio. • Elementos tales como patch cords, etiquetado, y de energía redundante requeridos para la conexión de los equipos suministrados.
1.4.	Monitoreo proactivo del servicio: el contratista monitoreará 7x24 la disponibilidad, capacidad, latencia, jitter y pérdida de paquetes del servicio (última milla y tramo hacia Internet), con generación de alertas y escalamiento según severidad. Evidencias disponibles para auditoría.
1.5.	Energía y condiciones eléctricas: el contratista verificará y certificará condiciones de alimentación (voltaje, tierra, protecciones) para los equipos instalados. Si se requieren adecuaciones estrictamente necesarias para la operación segura de los equipos suministrados, serán realizadas por el contratista sin costo adicional para la entidad, con informe técnico y aprobación de la supervisión.
1.6.	El servicio de internet para la Policía Nacional debe contener herramientas de monitoreo y análisis de tráfico de canal que permita supervisar en tiempo real la carga de tráfico de interfaces de red, así como también las mediciones de disponibilidad de canal y de los activos que soportarán la prestación del servicio. a) Proveer herramientas de observabilidad/NMS con licenciamiento a nombre de la Policía Nacional, que permitan visualización en tiempo real de utilización del canal, salud de equipos, disponibilidad, latencia y alarmas. b) Integración con mecanismos de exportación (API/CSV/syslog/SNMP/telemetría) para consumo por herramientas institucionales. c) Entrega de informe mensual (y a demanda del supervisor) con: disponibilidad, indisponibilidades, causas raíz, utilización de canal (picos/promedios), latencia/jitter/pérdida, cambios ejecutados, y plan de mejora.
1.7.	Revisión de seguridad y alineación con SGSI: el contratista realizará revisión inicial de la postura de seguridad del perímetro asociado al servicio, propondrá ajustes alineados con políticas institucionales, gestión del riesgo y normatividad aplicable, e implementará cambios aprobados por la Policía Nacional.
2	**SOLUCIÓN DE CANALES WLAN**
2.1.	El contratista realizará la instalación, configuración, conexión, adecuaciones físicas, obras civiles, instalación de dispositivos (routers, módems, otros) puesta en marcha y monitoreo de la última milla y cualquier otro componente necesario para la prestación del servicio en todas las sedes, descritas en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO". El servicio o punto de conexión, se debe entregar en un rack ubicado en el centro de datos o cuarto de redes en cada uno de los sitios de instalación descritos en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO" Los servicios de soporte en sitio, reemplazo o cambio de equipos o repuestos, servicios de gestión y demás costos asociados deben ser asumidos por el contratista, sin generar costos adicionales a la Policía Nacional.
2.2.	La solución debe tener la capacidad de transmitir voz, datos y video entre cada canal contratado y la sede principal en Bogotá, con la mejor tecnología brindada por el operador (MPLS y/o SD-WAN), con un ancho de canal sin reúso de acuerdo con los canales de datos descritos en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".

2.3.	El ancho de banda en la sede principal, ubicada en el Data Center de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, ubicada en Carrera 59 No. 26-21 CAN Bogotá D.C., será como mínimo la sumatoria de todos los anchos de banda de los sitios contratados.
2.4.	El contratista cubrirá todos los costos de los elementos como ductería, canalizaciones, cableado estructurado, sistemas de puesta a tierra, obras civiles necesarias para la instalación de los servicios contratados, sin modificar la estructura física de los sitios y reparar los daños presentados con ocasión del montaje de los equipos. Será responsabilidad del contratista verificar que en el sitio donde se instalarán los equipos, la corriente, el voltaje, los sistemas de puesta a tierra y demás elementos necesarios para tal fin, estén dentro de los parámetros mínimos requeridos para la operación de estos; en caso de requerirse, el contratista deberá realizar todas las adecuaciones necesarias para el funcionamiento del servicio. Por ningún motivo este punto será causal de retraso de la ejecución o cumplimiento del contrato, ni deberá generar costos adicionales a la Policía Nacional.
3	**ROUTER SITIO PRINCIPAL**
3.1.	El contratista deberá instalar en el Data Center de las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones, dos (02) Router que soportarán el canal principal y backup con las siguientes especificaciones mínimas: • Redundancia en alimentación eléctrica de dos (2) fuentes. • Throughput general de 20 Gbps. • Throughput por interfaz 10 Gbps. • Licenciamiento para tráfico cifrado de 20 Gbps. • Memoria de 8 GB DDR3. • Chasis integrado. • Seis (6) interfaces GigabitEthernet Ethernet Medio Fibra Óptica Modulo SFP • Dos (2) interfaces TenGigabit Ethernet. • Soportar protocolos de enrutamiento IPv4, IPv6, HSRP, BGP, VRF. • Soportar protocolo SNMP para la gestión de eventos. • Soportar Protocolo de cifrado túnel VPN GRE IPsec y SSL VPN. • Soportar Protocolo de cifrado IPSEC-AES256. • Control del tráfico entrante y saliente. • Control de calidad de servicio QoS. • Soporte con fabricante durante la duración del contrato. • Alta escalabilidad. • Instalación rackeable. El oferente debe anexar la ficha técnica del producto para validar las especificaciones técnicas mínimas solicitadas.
4	**ROUTER SEDES**
4.1.	El contratista deberá instalar para cada uno de los enlaces contratados en las diferentes sedes descritas en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO" un ROUTER con las siguientes características mínimas: • Dos (2) interfaces Gigabit Ethernet. • Soportar protocolos de enrutamiento IPv4, IPv6, HSRP, BGP, VRF. • Soportar protocolo SNMP para la gestión de eventos. • Soportar Protocolo de cifrado túnel VPN GRE IPSEC-AES256. • Control del tráfico entrante y saliente. • Soporte con fabricante durante la duración del contrato. • Licenciamiento para tráfico cifrado de acuerdo con el ancho de banda del enlace. • El Throughput de cada equipo deberá soportar el ancho de banda del canal instalado en la sede y debe estar en la capacidad de soportar mínimo un 30% de crecimiento. • Instalación rackeable. El oferente debe anexar la ficha técnica del producto para validar las especificaciones técnicas mínimas solicitadas.

5	SISTEMA DE SEGURIDAD PERIMETRAL
	UTM (UNIFIED THREAT MANAGEMENT- GESTIÓN UNIFICADA DE AMENAZAS)
5.1.	El contratista debe suministrar e instalar en el data center de la Policía Nacional, el hardware del UTM el cual debe contener mínimo cuatro (04) interfaces de red a 100 Gbps, catorce (14) interfaces de red a 10 Gbps, de la misma forma debe soportar protocolo IPv4 e IPv6 y los siguientes servicios como mínimo: • **Firewall de nueva generación** con módulos de control de navegación de cada uno de los usuarios, en caso que el reporteador no esté incluido con el firewall, se deberá incluir y personalizar de acuerdo a la necesidad de la institución, este debe contar con graficas en tiempo real del uso del canal, estadísticas sobre top ataques, top de sitios navegados, top de aplicaciones, top de conexiones, top de protocolos, deberá contar con un módulo web Gateway con un motor actualizado de categorías de navegación con capacidad de reportar y personalizar al detalle de sitio vs usuario, para el tema de usuarios deberá estar integrado con el administrador de identidades de la Policía Nacional (OID), previa autenticación con el LDAP y demás información que sea recopilada por el firewall, este sistema se deberá integrar al SIEM de la Policía Nacional, de igual forma deberá soportar como mínimo un throughput de 20 Gbps. • Antispyware y Antivirus, este sistema se deberá integrarse a la herramienta de administración de eventos e información de seguridad de la Policía Nacional. • IPS y administración de ancho de banda, este sistema se deberá integrarse a la herramienta de administración de eventos e información de seguridad de la Policía Nacional. • Realizar control por HTTP y HTTPS modo transparente en IPV4, IPV6 para filtrado de contenido. • El equipo deberá generar reportes, gráficas y estadísticas.
5.2.	El UTM debe ser entregado en alta disponibilidad con dos (02) equipos físicos en clúster, no se aceptan soluciones en la nube. El Contratista deberá garantizar el soporte y licenciamiento durante el tiempo de ejecución del contrato, sin generar costo adicional a la policía nacional.
5.3.	Se deberá suministrar el hardware, software y demás elementos físicos dimensionados con una capacidad mínima para soportar setenta y cinco mil (75.000) usuarios para lo cual, deberá permitir ochocientas mil (800.000) nuevas conexiones concurrentes por segundo y capacidad de conexiones TCP concurrentes de setenta millones (70.000.000). Además, debe estar compuesta del software necesario para realizar la conexión, comunicación y operación del servicio a internet, deben ser previstos el mejoramiento del nivel seguridad, basado en un sistema de gestión de seguridad de la información, esto no debe generar costos adicionales a la Policía Nacional.
	MÓDULO DE ESTADÍSTICAS VÍA WEB
5.4.	El contratista deberá proveer una herramienta independiente que permita el acceso seguro (usuario y password) a un módulo de estadísticas vía WEB sobre https, que incluya como mínimo lo siguiente: **Utilización del Canal:** • Estadística diaria, semanal y mensual de la utilización real del canal de internet – histograma. • Estadística acumulada (desde el primer día de inicio del contrato) de la utilización real del canal de internet – histograma • Estadística por periodo (seleccionado a criterio del operador desde el día _ hasta el día _) diaria de la utilización real del canal de internet – histograma. **Sitios WEB visitados:** • Estadística diaria de los top-10 de los sitios Web (paginas) más visitados. Se requiere que este informe se presente por IP origen, IP destino y nombre, diferenciamiento de tráfico tanto nacional (dentro del NAP Colombia) como internacional, local y de latencia de última milla. • Igualmente, para la semana, el mes, el acumulado desde el inicio del contrato, y por periodo desde fecha ____ hasta___. • Estadística del tráfico por protocolo, por dirección IP y diferenciamiento de tráfico tanto nacional como internacional **Consultas por usuario:** • Estadística diaria de los top-10 de los usuarios que más utilizan el servicio de internet. Se requiere que este informe se presente por tiempo en la red y por cantidad de Bytes transferidos y recibidos.

	• Igualmente, para la semana, el mes, el acumulado desde el inicio del contrato, y por periodo desde fecha __ hasta__. El contratista deberá configurar las plantillas necesarias que permitan obtener las estadísticas que requiera la institución.
	WAF (WEB APLICATION FIREWALL)
5.5.	La solución WAF deberá estar compuesta por dos componentes integrados: Un componente on-premise, el cual deberá ejecutarse sobre equipos físicos appliance instalados en el datacenter de la Policía Nacional. Y un componente en nube (CloudWAF), el cual deberá integrarse de forma nativa con el componente on-premise mediante API u otros mecanismos provistos por el fabricante. El componente on-premise del WAF deberá ejecutarse sobre los mismos equipos físicos appliance de la solución de balanceo de carga requerida en el numeral 5.6, sin requerir equipos dedicados o separados para prestar la funcionalidad de WAF local. En consecuencia, los appliances físicos ofertados para balanceo deberán soportar de manera nativa y simultánea las funcionalidades de balanceo de carga y configuración de CloudWAF. La solución debe permitir un mínimo de sesenta (60) servicios web publicados por la Policía Nacional con sesiones concurrentes HTTP y HTTPS en promedio de 1.900.000 **conexiones concurrentes** con un crecimiento del 30% y 4.000.000 de peticiones **por segundo** HTTP de capa 7, y un soporte mínimo de 2 Gbps de inspección de protección web total (WAF). La integración con el servicio de CloudWAF deberá ser vía API, sin requerir modificaciones de DNS ni necesidad de instalar certificados digitales por fuera de la red de la Policía Nacional, la decisión del bloqueo debe hacerse de acuerdo con la política del CloudWAF y el bloqueo debe hacerse local en los balanceadores. Esta solución deberá entregar reportes en tiempo real de los ataques bloqueados con detalles como IP y país del atacante, tipo de ataque, acción tomada, categoría de OWASP Top Ten Web, así como estadísticas en tiempo real con valores como top de ataques, top de tipos de ataque y top de aplicaciones afectadas, entre otras. Este sistema se deberá integrar con la herramienta de administración de eventos e información de seguridad con que cuenta la Policía Nacional. La solución deberá ser un componente que opere eficientemente para proteger las aplicaciones web de la Policía contra amenazas externas e internas, en una conexión activo/activo. La solución deberá contar con una interfaz gráfica que permita implementar controles basado en políticas hacia los servidores web de la Entidad. La solución deberá permitir el monitoreo de la actividad de todo el tráfico sobre HTTP y HTTPS de los servicios web de la Entidad. La solución deberá incluir un servicio de soporte 7x24x365 brindado por fabricante, que proveerá asistencia durante la fase de onboarding de las aplicaciones y la gestión de incidentes durante la duración del contrato. Deberá incluir un Customer Success Manager asignado a la cuenta. **Protección contra ataques Web** La solución deberá contar con políticas de seguridad que soporten modelos de seguridad positivos y negativos. Protección de ataques de SSRF, RFI, contra comandos de SQL, comandos de shell y ataques de cross-site scripting, Cross Site Scripting (XSS), SQL Injections, Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Backdoor, prevención de defacement, control de fuga de información, source blocking (cuarentena) por actividad sospechosa recurrente, bloqueo por reputación del atacante, detección de ataques del lado del cliente, para proteger contra amenazas de formjacking, Megacart, supply chain,e-skimming y DOM based XSS.

	Protección contra Bots La solución incluir protección contra ataques de tipo BOT (ataques automatizados) basado en firmas, con mitigación mediante captcha. **Punto de Presencia (POP)** La solución debe contar con POP (Point of Presence) en Colombia, con el fin de que se presente un rendimiento optimo en las peticiones, reduciendo la latencia en la entrega de paquetes y mejorando la velocidad de transferencia de forma eficiente.
	SOLUCIÓN DE BALANCEO DE CARGA
5.6.	Se debe incluir una solución de balanceadores que este en alta disponibilidad, que cuente mínimo con las siguientes características: • Soportar como mínimo 10 Gbps de throughput en capa 7 cada una de los appliances. Y una capacidad de 2500 RPS SSL con llaves RSA de 2048 bits • Cada balanceador debe soportar escalar hasta 32 instancias de balanceo. Se deben incluir al menos 5 instancias por balanceador. • La solución debe incluir conectividad a 10 GbE para mínimo puertos con conexión para fibra multimodo por cada balanceador. • La solución de balanceo deberá soportar de manera nativa la habilitación y ejecución de la funcionalidad de WAF sobre los mismos appliances físicos ofertados, sin requerir equipos independientes para el componente WAF on-premise. • Los equipos físicos ofertados como balanceadores de carga deberán ser los mismos equipos físicos sobre los cuales operará el componente on-premise de la solución WAF descrita en el numeral 5.5. • La solución de balanceo debe soportar la capacidad de habilitar la tecnología de caching para los servicios Web balanceados, y debe permitir asignar recursos físicos independientes para la funcionalidad de optimización de desempeño Web (WPO), para evitar que el balanceador y el caching/WPO compartan los mismos recursos. • La solución de balanceo debe permitir definir una dirección IP específica (NAT) como el origen de los chequeos de salud. • La solución de balanceo debe soportar balanceo transparente, en donde se realicé inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original. • La solución de balanceo debe permitir filtrar el tráfico capa 2 que no esté relacionado a frames IP. La solución debe soportar el protocolo de encriptación TLS 1.3 y criptografía post-quantum como (híbrido y FIPS-203)
5.7.	El contratista deberá entregar una solución de balanceo de carga, de sitios, enlaces y DDoS, de la misma marca del WAF ofertado, instalada en el data center de la Policía Nacional y operando en alta disponibilidad. Adicionalmente, deberá quedar expresamente establecido que el componente on-premise del WAF se ejecutará en los mismos equipos físicos appliance de la solución de balanceo de carga ofertada, correspondiendo a una misma plataforma física con capacidades integradas de balanceo y protección WAF, complementada por un componente CloudWAF en nube del mismo fabricante.
	SERVICIO DE MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS DISTRIBUIDOS (DDoS por sus Siglas en Ingles) en sitio
5.8.	Dispositivo de mitigación de ataques DDoS, mediante equipo físico ubicado en el datacenter de la Policía Nacional, el cual deberá contar con actualización durante la ejecución del contrato para la herramienta, con la última versión liberada por el fabricante, sin generar costo adicional a la Policía Nacional.

LUGAR	UBICACIÓN	TRÁFICO LEGÍTIMO	MITIGACIÓN	ÚLTIMA MILLA
Policía Nacional	Dirección General Carrera 59 No. 26-11 CAN Edificio OFTIC Bogotá Colombia	10 Gbps	20 Gbps	Fibra Óptica

	• **La solución AntiDDoS en sitio se debe integrar de manera nativa con los demás componentes a adquirir (balanceador de carga, WAF, servicio de mitigación DDoS en nube y consola de gestión) y debe garantizar la protección y el despliegue de las aplicaciones durante el período de transición, en el cual, se debe tener en cuenta que actualmente dicha solución es de la marca Radware. Esta integración permite mitigar ataques avanzados dirigidos a las aplicaciones y evitar puntos ciegos en los procesos de detección y mitigación de amenazas.** • La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos. • Debe contar con una tasa de prevención de ataques mínima de 14 Mpps. • El máximo de sesiones concurrentes debe ser ilimitado. • La solución debe contar con la capacidad de integrarse con el correlacionador de eventos SIEM (Security Information and Event Management) con el que administre la Policía Nacional. • La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener los ataques 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 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 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 sensibilidad 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 debe detectar y mitigar ataques entrantes y salientes de denegación de servicio. • La solución debe integrarse de manera nativa con la solución de ataques antiDDoS que se encuentra en la nube del proveedor
5.9.	Se debe incluir una consola de gestión centralizada de tal forma que administre la solución WAF, de Balanceo y de mitigación de ataques de denegación de servicios distribuidos (DDoS) El servicio debe disponer de un portal que contenga por lo menos las siguientes características: • Autogestión para los usuarios • Múltiples cuentas de usuarios con capacidad de personalizar vistas • Alertas operacionales en el portal, SMS y por e-mail • Alertas de seguridad en el portal, SMS y por e-mail • Capacidad de configurar los anchos de banda y tiempos críticos para desvió de tráfico • Estadística de tráfico entrante al Scrubbing Center • Estadísticas de tráfico legítimo • Estadísticas de tráfico entrante en el equipo instalado en la Entidad • Reportes Gerenciales • Reportes de incidentes.
SERVICIO DE MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS DISTRIBUIDOS (DDoS por sus Siglas en Ingles) en la nube	
5.10.	**El contratista deberá proveer adicionalmente un servicio de Mitigación de ataques DDoS basado en Nube que se integre de manera directa con los demás componentes a adquirir (balanceador de carga, WAF, servicio de mitigación DDoS en sitio y consola de gestión), sin el uso de equipos o software intermediario o adicional, asegurando un despliegue y funcionamiento fluido y estable, garantizando la implementación de políticas de seguridad institucionales durante todo el proceso de transición.** • El servicio ofrecido debe desplegarse completamente en nube e integrarse con la infraestructura actual de la Policía Nacional. • El servicio debe permitir 20 Gbps de tráfico legítimo y la protección de hasta 126 direcciones IP públicas (DNS) • **La solución AntiDDoS en nube se debe integrar de manera nativa con los componentes a adquirir (servicio de mitigación DDoS en sitio y consola de gestión), garantizando la protección y despliegue de aplicaciones durante el periodo de transición, en el cual, se debe tener en cuenta que actualmente dicha solución es de la**

	marca Radware. Esto permite que se mitiguen ataques avanzados de aplicación y no se tengan puntos ciegos en la mitigación y detección de ataque.
5.11.	El servicio se debe prestar para mitigar ataques ilimitados mensuales con duración ilimitada
5.12.	El servicio debe contar con protección a ataques tipo Burst, desde IPs dinámicas, ataques DNS y otros.
5.13.	El servicio debe poder alertar de los ataques por email, SMS, API, o por un Portal WEB
5.14.	El servicio no debe sumar latencia al tráfico legitimo. Es decir, cuando no hay un ataque activo el tráfico no debe ser manipulado y debe ser entregado directamente sin retardos de comunicación.
5.15.	Se debe incluir la instalación y configuración del Servicio de protección DDoS en Nube y del equipo físico en las instalaciones de Policía Nacional.
5.16.	El contratista deberá seguir en todo momento durante el desarrollo del contrato las especificaciones de seguridad de conformidad con las políticas de seguridad del Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, Resolución 04408 del 26/12/2024; el cual se suministrará al contratista que le sea adjudicado el presente proceso.
	SOPORTE PARA SEGURIDAD PERIMETRAL
5.17.	**El contratista deberá disponer de un (1) ingeniero de soporte contratado de manera directa y exclusiva para seguridad perimetral del contrato con disponibilidad de 7x24, el cual debe asistir a las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones de la Dirección General ubicada en la carrera 59 Nro. 26 – 21 CAN, en el horario de 8:00 am a 12:00 m y de 2:00 pm a 6:00 pm.** Este ingeniero debe contar con certificación directa de los fabricantes de los equipos de seguridad presentados.
6	**SERVICIO DE WIFI**
6.1.	Garantizar el acceso WLAN y la conectividad LAN/WLAN para proveer los servicios de comunicación de voz, datos y video, para todos los usuarios de la Policía Nacional que requieran de estos servicios, de acuerdo al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".
6.2.	La Policía Nacional cuenta con la infraestructura de cableado estructurado, la cual podrá ser usada para la instalación de los equipos requeridos por el contratista y así cumplir con lo descrito en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO". No obstante, de requerirse nueva infraestructura o mantenimiento correctivo del cableado de datos y eléctrico existente, que sea necesario para garantizar la conectividad, el contratista deberá realizarlos, sin generar costos adicionales a la Policía Nacional de Colombia. El contratista deberá generar las visitas necesarias para el mantenimiento correctivo a solicitud del supervisor del contrato sobre el cableado existente y solventar las fallas que afecten el servicio de WIFI. Es de aclarar que las visitas son dirigidas a las unidades de Policía en donde se presenten las fallas en el cableado del anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO", sin generar costos adicionales a la Policía Nacional de Colombia.
6.3.	Diseñar la infraestructura, aprovisionar, instalar, configurar, probar y mantener los equipos activos relacionados con la solución LAN inalámbrica (WLAN), con su correspondiente mantenimiento preventivo y correctivo durante la vigencia del contrato.
6.4.	Para cada unidad descrita en al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO", el contratista debe realizar el diseño detallado en capas de la solución LAN-WLAN a implementar para prestar un eficiente servicio, este deberá ser aprobado por el supervisor del contrato.
6.5.	Instalar, configurar, administrar y gestionar todos los componentes LAN y WLAN para el funcionamiento de los mismos. En los casos donde el canal de datos instalado en cada unidad descrita en al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO", sea suministrado por otro proveedor de servicios, el contratista deberá realizar las respectivas gestiones necesarias para garantizar el funcionamiento extremo a extremo de la solución WLAN, sin generar costos adicionales a la Policía Nacional.
6.6.	Atender los eventos que se presenten con la LAN, WLAN que hacen parte del servicio.
6.7.	Los access point a implementar deberán estar en la capacidad de permitir y soportar su gestión centralizada en la nube u on-premise o híbrida, como mínimo una controladora. La gestión y/o administración de la solución estará a cargo del contratista, no obstante, será de forma compartida con los funcionarios de Policía designados, los cuales recibirán por parte del contratista entrenamiento en el manejo de las herramientas.
6.8.	El servicio debe prestarse sobre una base de operación 7x24x365.
6.9.	Se deberá prestar el servicio de mantenimientos preventivos programados a los diferentes equipos y del sistema en general durante el tiempo del contrato, para lo cual el contratista deberá generar un cronograma de la ejecución de los mantenimientos, previa aprobación del supervisor del contrato.

6.10.	Se deberá prestar servicio de mantenimiento correctivo de los equipos del contratista en caso necesario una vez realizado diagnóstico: cuyas actividades estarán orientadas hacia la restitución de las características de funcionamiento de los equipos o sistema después de ocurrida la falla; dichas actividades estarán a cargo de la empresa prestadora de servicio, incluyendo todos los repuestos originales, nuevos, genuinos, no re manufacturados que sean necesarios para el correcto funcionamiento de los equipos y servicio objeto de este contrato; además la mano de obra, la garantía de los repuestos y la calidad del mantenimiento serán objeto aprobación previo concepto de satisfacción del supervisor del contrato antes de instalar algún repuesto.
6.11.	El contratista deberá estar en la disponibilidad de prestar asistencia técnica 7x24x365, durante la vigencia del contrato.
6.12.	En caso de tener un equipo que posterior a diagnóstico necesite ser reemplazado, el tiempo máximo de atención por parte del contratista para el cambio del equipo será de máximo 48 horas. El tiempo que se deje de prestar el servicio por daño de los dispositivos, contará dentro de las indisponibilidades.
6.13.	El contratista presentará un gerente de proyecto el cual debe estar contratado de manera directa por la firma que le sea asignado el contrato, quien estará como enlace entre la Policía Nacional y el contratista, para atender los requerimientos técnicos y administrativos necesarios, durante la vigencia del contrato. El contratista dispondrá de mínimo un ingeniero de soporte en sitio contratado de manera directa para el soporte del servicio de WIFI, en las instalaciones de la Oficina de tecnologías de la Información y las comunicaciones de la Dirección General en un horario comprendido de lunes a viernes en horarios de 8 a 12 y de 2 a 6 PM.
6.14.	El contratista entregará mensualmente un reporte en formato digital del uso del servicio al supervisor del Contrato, y al Jefe del Grupo de Tecnologías de la Información y las Comunicaciones de la Dirección de Educación Policía (DIEPO); donde se indique como mínimo las cantidades máximas de usuarios conectados a la red WiFi, las fallas que se están presentando y el motivo si lo hubiera, por cada colegio y escuela de formación de la Policía Nacional donde sea instalada la solución.
6.15.	Ejecutar las obras civiles "SI" son necesarias para el aprovisionamiento del servicio LAN/WLAN, incluyendo las relacionadas con la instalación de cableado estructurado, cableado eléctrico regulado, canaletas, estas deben cumplir las normas que garanticen la estética y la funcionalidad. (Canalizaciones, soportes, repisas, protecciones de intemperie, resanes, rompimiento de muros y pisos, bases para instalación de equipos, entre otros), sin generar costo adicional a la Policía Nacional.
6.16.	El contratista deberá realizar el diseño o estudio para cumplir con las necesidades de conectividad WLAN en las sedes de la Policía Nacional de acuerdo al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".
6.17.	El contratista deberá suministrar los equipos de comunicaciones que hacen parte de la solución, incluyendo switches, access points, controladora de access points y demás equipos necesarios para la prestación del servicio, sin generar costo adicional a la Policía Nacional.
6.18.	El contratista deberá suministrar, instalar y configurar los equipos activos que hacen parte de la solución en las sedes de la Policía Nacional de acuerdo al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".
SWITCHES DE ACCESO	
6.19.	Los switches de acceso deberán cumplir con las siguientes características mínimas:
6.20.	Equipos administrables con puertos Ethernet para acceso de usuarios y equipos finales, con capacidad mínima de 1Gbps por puerto; se deberá permitir multigigabit (2.5Gbps/5Gbps) cuando el diseño WLAN lo requiera. El número de puertos Ethernet deberá ser el requerido para la puesta en funcionamiento de la solución, conforme al anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO", incluyendo crecimiento y reservas operativas.
6.21.	Cuatro (04) puertos en fibra óptica para la conexión al switch de Core/Distribución con velocidad mínima de 10Gbps (SFP+); se aceptan velocidades superiores (25Gbps) si el diseño lo requiere. El contratista deberá suministrar los módulos transceiver y patch cords necesarios, compatibles con los equipos a instalar por el contratista y con los existentes en las sedes de la Policía Nacional, garantizando interoperabilidad y operación estable.
6.22.	Soporte de configuración de mínimo 4000 VLANs, incluyendo funciones asociadas a segmentación y operación al igual que soporte de troncales 802.1Q.
6.23.	La posibilidad de limitar el acceso a la red con base en las direcciones MAC, mediante mecanismos de Port Security (máximo de MAC por puerto, sticky MAC, acciones ante violación), y controles complementarios de acceso tales como 802.1X con autenticación centralizada (RADIUS/TACACS+ o equivalente), según aplique al diseño institucional.
6.24.	Los suficientes puertos con soporte PoE para alimentar los access points y otros dispositivos que lo requieran, cumpliendo como mínimo PoE+ (IEEE 802.3at); cuando el diseño WLAN lo exija, el switch deberá soportar PoE++ (IEEE 802.3bt Tipo 3/4). El contratista deberá indicar el presupuesto PoE total (W) y por puerto, asegurando alimentación simultánea para la cantidad de AP previstos por sede. En caso excepcional de no contar con PoE disponible en un punto específico, los Access Point podrán ser alimentados por Power Injector, el cual deberá ser suministrado por el contratista, dimensionado y certificado para el AP correspondiente, sin costo adicional.

	SWITCHES DE DISTRIBUCIÓN
6.25.	Los switches de distribución deberán cumplir con las siguientes características mínimas:
6.26.	Soportar Bridges and Bridged Networks (IEEE 802.1Q) y operación con IPv4 e IPv6 (doble pila). Adicionalmente, deberá soportar mecanismos de protección y control de capa 2 para evitar bucles y tormentas de broadcast/multicast/unicast (storm control o equivalente)
6.27.	Deberán ser Capa 3 (del modelo OSI) y soportar protocolos de enrutamiento OSPF, RIPv1, RIPv2 o similares, y rutas estáticas.
6.28.	Permitir el enrutamiento inter-VLAN (SVI) y políticas de control de tráfico entre VLAN mediante ACL para IPv4 e IPv6 (o mecanismo equivalente), con trazabilidad y administración centralizada cuando aplique.
6.29.	Asignación dinámica de VLAN, soportando integración con mecanismos de autenticación 802.1X/RADIUS o equivalente, cuando sea requerido por la política institucional de control de acceso.
6.30.	Estar en capacidad de detectar y proteger contra ataques de ARP mediante mecanismos como Dynamic ARP Inspection (DAI) o equivalente, y controles de suplantación de IP/MAC cuando aplique al diseño.
6.31.	Tener la cantidad de puertos suficientes para conectar a través de fibras ópticas el cableado vertical de las sedes. La velocidad de las interfaces de fibra deberá ser de por lo menos 10 Gbps (SFP+); se aceptan velocidades superiores si el diseño lo requiere. El contratista deberá suministrar los módulos transceiver y accesorios necesarios, compatibles con los equipos a instalar por el contratista y con los instalados en las sedes de la Policía Nacional, garantizando interoperabilidad y operación estable.
	SWITCHES DE CORE
6.32.	Mínimo veinticuatro (24) puertos 100/1000 Base T, PoE+ (802.3at), en todos sus puertos RJ45.
6.33.	Mínimo cuatro (04) Puertos 1/10GbE SFP+, totalmente independientes, no compartidos. Para las interconexiones de backbone, el contratista deberá suministrar por cada equipo módulos transceiver SFP+ de 10 Gbps con conector LC, así: Dos (02) módulos monomodo compatibles con fibra óptica OS2 y frecuencia de onda de 1310 nm, distancia máxima 10 Km. Dos (02) módulos multimodo compatibles con fibra óptica OM4 y frecuencia de onda de 850 nm, distancia 400 mt. **Los módulos o transceptores ópticos podrán ser suministrados directamente por el fabricante de los switches o estar oficialmente aprobados o soportados para su uso con los equipos ofertados. En todos los casos, el contratista deberá garantizar su compatibilidad con las interfaces, velocidades y arquitectura de origen y destino, así como la interoperabilidad, estabilidad, soporte y garantía integral de la solución durante la vigencia contractual, sin generar costos adicionales para la Policía Nacional.**
6.34.	Administrables vía CLI, web y/o HTTP, SSH v2.0.
6.35.	Instalación rackeable de diecinueve (19) " y 1 UR.
6.36.	Capacidad 128 Gbps (Switching) / 42 Mpps (Reenvío)
6.37.	Funciones L3 Enrutamiento Estático, RIP, RIPng y OSPF
6.38.	Gestión de Red CLI (Consola), Web, SNMP (v1/v2c/v3), SSH v2
6.39.	Stacking mínimo para ocho (08) switch incluyendo la totalidad de licenciamiento necesario para su configuración.
6.40.	Certificación en Seguridad UL60950-1 y/o EN62368-1
6.41.	Certificación ambiental ROHS y/o WEEE y/o REACH.
6.42.	Estándar de eficiencia energética IEEE 802.3az y/o ETSI.
6.43.	Gestión y protocolos IPV4, IPv6 (RFC2460), ACL para IPv4, ACL para IPv6 y/o Firewall Filters para IPv6
6.44.	Puerto de consola / management Un (1) Puerto RJ45 y/o Un (1) Puerto USB y/o Un (1) Puerto USB tipo C.
6.45.	Manejo de Vlan mínimo 4000
6.46.	Alimentación 100 - 120 VAC, frecuencia 50 / 60 Hz
	LAN INALÁMBRICA (WLAN)
6.47.	La solución mediante la que se preste el servicio debe ser robusta, adecuada a las necesidades de funcionamiento, cobertura y capacidad de la Policía Nacional. El servicio debe prestarse con igual calidad y continuidad para todas las sedes, considerando escenarios de alta densidad (aulas, auditorios, zonas comunes), y deberá permitir escalabilidad sin reemplazo total de la plataforma.
6.48.	La solución debe soportar el uso de túneles GRE o IPSec. Adicionalmente, deberá soportar transporte seguro de tráfico de gestión y/o datos cuando aplique al diseño, con cifrados vigentes y sin degradación significativa del servicio.
6.49.	Debe soportar e implementar protocolos y controles de seguridad, como mínimo: cifrado robusto de la red inalámbrica, segmentación por SSID/VLAN, aislamiento de clientes cuando aplique, y administración segura (HTTPS/SSH, control de roles y auditoría de cambios).

6.50.	Permitir la autenticación de usuarios y la prevención contra intrusos. Como mínimo deberá soportar autenticación empresarial mediante 802.1X/RADIUS (o equivalente) y contar con capacidades de detección/prevención de intrusos inalámbricos (WIDS/WIPS o equivalentes), con generación de alertas y reportes.
6.51.	Soportar la autenticación por MAC. Esta funcionalidad deberá operar como mecanismo complementario (lista blanca/negra, perfiles por dispositivo) y permitir políticas de control por tipo de dispositivo, sin limitar la implementación de autenticación empresarial.
6.52.	Los Access Point´s deben soportar banda dual simultánea. Adicionalmente, deberán soportar direccionamiento y operación concurrente según el diseño (2.4 GHz, 5 GHz; y, cuando sea viable, 6 GHz para Wi-Fi 6E), con selección inteligente de banda (band steering o equivalente).
6.53.	Cumplir con IEEE 802.11e o equivalente, implementado mediante Wi-Fi Multimedia (WMM/EDCA), para brindar Calidad de Servicio (QoS) y priorización de tráfico de voz y video. En seguridad, la solución deberá soportar el marco IEEE 802.11i (RSN) y operar como mínimo con autenticación empresarial 802.1X, privilegiando WPA3-Enterprise; se permitirá WPA2-Enterprise únicamente como modo de compatibilidad/controlado para equipos legados. Para WPA3-Enterprise se deberá soportar y habilitar Protección de Tramas de Gestión (PMF/802.11w), y cuando se opere en banda de 6 GHz (Wi-Fi 6E/7) deberá cumplirse el requisito de WPA3 y PMF, sin permitir WPA2 en dicha banda, garantizando la priorización de voz y video.
6.54.	Soportar los estándares IEEE 802.11b/g/n/ac/ax y el IEEE 802.3 aplicable según las interfaces utilizadas o los de mejor especificación en el momento de instalación. Para nuevas implementaciones, se privilegiará 802.11ax (Wi-Fi 6) y, cuando aplique, Wi-Fi 6E; los equipos deberán soportar funciones de eficiencia para alta densidad (OFDMA, MU-MIMO o equivalentes).
6.55.	Ofrecer la funcionalidad de roaming que permita conservar la dirección IP, políticas de seguridad, VLAN y ACL del dispositivo usuario mientras se encuentre en roaming, garantizando la continuidad de los servicios de voz y datos al usuario. Adicionalmente, deberá soportar mecanismos de roaming rápido (802.11k/v/r o equivalentes) para minimizar cortes perceptibles.
6.56.	Proveer los servicios de autenticación, autorización y protección contra intrusos tales como un Portal Cautivo o equivalente que impida el ingreso sin los controles de seguridad mínimos necesarios.
6.57.	Contar con mecanismos de auto recuperación que permitan dar continuidad del servicio y ampliación de cubrimiento de access points adyacentes en caso de falla de uno de ellos. Adicionalmente, la solución deberá permitir re-balanceo automático de clientes y re-asignación dinámica de canales/potencia para mantener desempeño.
6.58.	Con relación a la distribución de usuarios debe soportar balanceo de cargas en forma dinámica entre access points para que el usuario inalámbrico tenga un mejor tiempo de respuesta. El balanceo deberá considerar métricas como RSSI/SNR, utilización de canal y número de clientes (o equivalentes).
6.59.	Autenticación de puntos de acceso inalámbrico mediante el uso de certificados y políticas de seguridad. La solución deberá permitir control de APs autorizados, detección de APs rogue y aplicación de políticas de mitigación/alertamiento.
6.60.	Soporte de direccionamiento IPv4 e IPv6 en toda la solución. La operación dual-stack deberá ser transparente para el usuario y administrable, incluyendo servicios de red asociados (DNS/DHCP según aplique).
6.61.	La solución inalámbrica deberá ser escalable en todos sus componentes, tanto en software como hardware, que permita realizar actualizaciones y crecimiento (capacidad de usuarios/APs/licencias) sin re-arquitectura completa.
6.62.	La solución debe estar acompañada de todos los accesorios necesarios para la operación de los equipos, tales como: software, cables de consola, cables de energía eléctrica, documentación técnica y manuales que contengan información suficiente para posibilitar la instalación, configuración, operación y soporte de la solución WLAN.
6.63.	Utilizar listas de control de acceso (ACL): Para los equipos que lo soportan, se deberán configurar ACL para IPv4 e IPv6, aplicables por SSID/VLAN/rol de usuario (cuando aplique), orientadas a segmentación, control de acceso y reducción de superficie de ataque. Las ACL deberán permitir: (i) control de tráfico entre redes (inter-VLAN/SSIDs), (ii) restricción por servicios/puertos/protocolos mínimos necesarios, (iii) control de acceso a redes de gestión, y (iv) registro (logging) y trazabilidad de cambios conforme al esquema de coadministración y auditoría.
6.64.	Soportar y operar con mecanismos de cifrado y autenticación vigentes para WLAN empresarial: WPA3-Enterprise (802.1X) como línea base; se permitirá WPA2-Enterprise únicamente como compatibilidad controlada para dispositivos legados. Para WPA3-Enterprise deberá soportarse y habilitarse Protección de Tramas de Gestión (PMF/802.11w). En caso de operar en banda 6 GHz (Wi-Fi 6E/7), el servicio deberá cumplir con los requisitos de WPA3 y PMF, sin permitir WPA2 en dicha banda.
6.65.	Los DNS del contratista deben estar en la capacidad de atender las peticiones DNS provenientes de la red WLAN a implementarse dentro de las escuelas de formación y los colegios de la Policía Nacional, considerando que el servicio utiliza DNS públicos y no los internos de la Policía Nacional. El servicio DNS deberá: (i) operar con alta disponibilidad, (ii) soportar resolución para clientes IPv4 e IPv6, (iii) permitir políticas de seguridad y control (por ejemplo: listas de permitidos/bloqueo por categorías o dominios, cuando aplique), (iv) contar con registro de eventos y evidencias para

	soporte/auditoría, y (v) garantizar tiempos de respuesta y continuidad del servicio conforme al esquema de operación 7x24 del WLAN.
	CONTROLADORA
6.66.	La controladora suministrada por el contratista deberá contar con redundancia y garantizar una disponibilidad mínima del 99.99%. En caso que la controladora no se encuentre en las instalaciones de la Policía Nacional, el contratista deberá garantizar el colocation y cross conexión entre el Datacenter del contratista y el Datacenter de la Policía Nacional, sin generar costos a la Policía Nacional, asegurando conectividad segura y continuidad del servicio.
6.67.	Soportar y permitir configurar mecanismos de cifrado y autenticación vigentes para WLAN empresarial desde la controladora: WPA3-Enterprise (802.1X) como línea base; se permitirá WPA2-Enterprise únicamente como modo de compatibilidad controlado para equipos legados. La controladora deberá soportar y permitir habilitar Protección de Tramas de Gestión (PMF/802.11w) para redes WPA3-Enterprise; y cuando se opere en banda 6 GHz (Wi-Fi 6E/7) deberá garantizar el cumplimiento de WPA3 y PMF, sin permitir WPA2 en dicha banda.
6.68.	La solución debe permitir cambiar el SSID (Service Set Identifier) y tanto habilitar como deshabilitar el broadcast, así como asociar parámetros de seguridad, VLAN/QoS por SSID según el diseño aprobado.
6.69.	La solución debe permitir múltiples definiciones de SSID (mínimo 8 por punto de acceso inalámbrico) para aceptar varias configuraciones, con diversas políticas de seguridad y calidad de servicio, permitiendo aplicar perfiles diferenciados con segmentación por VLAN y controles de acceso asociados cuando aplique.
6.70.	La solución debe soportar el uso de túneles GRE o IPsec, cuando el diseño lo requiera, para transporte seguro de tráfico/gestión entre sedes o hacia el punto de control definido, garantizando continuidad del servicio.
6.71.	Deberá contar con software que le permita adaptarse y administrar en tiempo real el entorno de RF. Entre estas funciones deberá encontrarse: • Asignación dinámica de canales para optimizar la cobertura y desempeño. • Balanceo de carga de usuarios entre múltiples puntos de acceso inalámbricos. • Detección y corrección de huecos en la cobertura inalámbrica. • Control dinámico de potencia de acuerdo a las condiciones de la red.
6.72.	La solución debe ser centralizada y deberá tener controlador alterno (cluster), si el controlador WLAN falla, los access points afectados deberán asociarse al secundario de forma automática, evitando que la red wireless se vuelva inoperativa.
6.73.	El controlador debe permitir el almacenamiento de la configuración en memoria no volátil, permitiendo recuperar la configuración en caso de falla eléctrica.
6.74.	La solución deberá incluir funciones de Cliente Radius aplicado al LDAP existente para la autenticación de los clientes Wireless en un servidor Radius centralizado.
6.75.	La controladora deberá proporcionar visibilidad en tiempo real del estado de los AP (en línea/fuera de línea), estado de radios, canales, potencia, utilización, clientes asociados, eventos/alertas y salud del enlace, con tableros y alertas operacionales para soporte.
6.76.	La solución deberá soportar análisis de espectro o capacidades equivalentes para identificar interferencia 802.11 y no-802.11 (no Wi-Fi) y habilitar acciones correctivas como planeación óptima de canal, ajuste automático de potencia, y medidas de mitigación basadas en evidencia. Adicionalmente, para entornos de alta densidad deberá soportar mecanismos de eficiencia/mitigación de interferencia propios de 802.11ax, manteniendo operación estable en anchos de canal configurados.
6.77.	Deberá implementar QoS basado en 802.11e/WMM (EDCA) o equivalente, con priorización por categorías (Voz, Video, Best-Effort y Background) y capacidad de clasificación/marcación para mantener la prioridad extremo a extremo, garantizando continuidad de servicios de voz y video en movilidad.
6.78.	La controladora deberá generar reportes y exportables (por portal o formato interoperable) que incluyan como mínimo: consumo por usuario, consumo por SSID/VLAN, utilización por AP/radio, tendencias por hora/día/mes, top clientes, y reportes de incidentes/alertas que soporten auditoría y seguimiento del servicio.
	ACCESS POINT – AP
6.79.	La solución implementada debe tener autonomía respecto a la controladora; es decir, los AP no deben depender para su funcionamiento de la controladora y deberán contar con supervivencia propia para que, en caso de falla de la controladora, estos sigan operando con normalidad, preservando la conectividad WLAN básica y las políticas previamente aplicadas según el diseño aprobado.
6.80.	Los Access Point debe soportar los estándares IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (Wi-Fi 6E), y 802.11be (Wi-Fi 7), incluyendo funcionalidades como Multi-Link Operation (MLO), 4KQAM, y canales de 320 MHz. Además, debe cumplir con estándares de gestión de red (802.11k/r/v), seguridad (802.11i), y calidad de servicio (802.11e)

6.81.	Proporcionar monitoreo de rendimiento inalámbrico actual, incluyendo visibilidad del estado del AP y sus radios, utilización del canal, clientes asociados, eventos/alertas y métricas de desempeño disponibles para operación, soporte y auditoría.
6.82.	Los Access Point deben ser high density, soportar balanceo de cargas por número de usuarios por AP y por utilización de ancho de banda de red inalámbrica; adicionalmente deberán soportar funciones de eficiencia para entornos densos propias de Wi-Fi 6/6E o equivalentes.
6.83.	Los Access Point deben permitir la conexión a través de la red existente utilizando los switches y cableados existentes. En caso que el switch/cableado existente no sea compatible con la solución (por capacidades de velocidad, PoE o interfaces), el contratista deberá proveer los elementos necesarios para conectarse a la red y garantizar operación estable, sin costo adicional.
6.84.	El proponente deberá adjuntar el Certificado de Interoperabilidad emitido por la Wi-Fi Alliance para los modelos de Access Points y Controladoras ofertados. Dichos certificados deben validar explícitamente el soporte para: Wi-Fi Multimedia (WMM), WPA3-Enterprise y Voice-Enterprise (que incluye 802.11r/k/v). No se aceptarán hojas de datos (Datasheets) como sustituto de la certificación oficial."
6.85.	Todos los equipos que conforman la solución WLAN (Access Points y Controladoras), deberán garantizar altos estándares de seguridad y protección de la información, acreditando como mínimo **una (1) de las siguientes certificaciones o estándares internacionales equivalentes**: • **FIPS 140-2 o FIPS 140-3** (Federal Information Processing Standards). • **Common Criteria (ISO/IEC 15408)** con nivel de aseguramiento **EAL2 o superior**. • **Certificación de cumplimiento con PCI Data Security Standard (PCI DSS)** para la arquitectura de red propuesta. • **FedRAMP** (Federal Risk and Authorization Management Program) o cumplimiento demostrado con la norma **ISO/IEC 27001** para la plataforma de gestión en la nube. • **Certificación del Esquema Nacional de Seguridad (ENS)** o estándares de seguridad de infraestructura crítica homologables en la región.
6.86.	Los puntos de acceso deberán tener características de auto calibración por cambio en la potencia y canales de transmisión, así como de poder auto corregir la pérdida de señal en un área por falla de un punto de acceso.
6.87.	Los puntos de acceso deben ser capaces de operar en frecuencias de 2.4 GHz, 5 GHz y 6 GHz simultáneamente, además soportar o realizar un barrido de frecuencia continúa programada o sobre demanda, identificando puntos de acceso o clientes irregulares.
6.88.	Los puntos de acceso deben soportar 200 usuarios por radio en sus tres bandas (2.4 GHz, 5 GHz y 6 GHz), para un total de 600 usuarios.
6.89.	El tráfico que viaja entre los Access point (AP) y el controlador debe ser encriptados.
6.90.	Se requiere que la solución técnica cuente con diferentes opciones de access point, que permitan cubrir los diferentes escenarios que tiene la Policía en todo el País.
6.91.	El equipo debe contar con indicadores de estado y actividad.
	ACCESS POINT INDOOR
6.92.	Las características técnicas deben ser las misma de los **ACCESS POINT – AP** salvo las que se especifiquen a continuación.
6.93.	Los puntos de acceso para interiores deben ser capaces de utilizar técnicas como agregación de canales o channel bonding y Múltiple Entrada-Múltiple Salida (MU-MIMO) de 4x4 enlace ascendente y descendente.
6.94.	Los puntos de acceso para interiores deberán garantizar una alta capacidad de gestión de clientes y ancho de banda, cumpliendo con **una (1) de las siguientes configuraciones mínimas**: • **Opción A (Enfoque en Densidad - Wi-Fi 6/6E):** Equipos con estándar IEEE 802.11ax (Wi-Fi 6 o 6E) que cuenten con tecnología MU-MIMO de **4x4 flujos espaciales (4x4:4)** tanto en enlace ascendente (UL) como descendente (DL) en la banda de 5 GHz. • **Opción B (Enfoque en Tecnología de Punta - Wi-Fi 7):** Equipos con estándar IEEE 802.11be (Wi-Fi 7) que cuenten con tecnología MU-MIMO de al menos **2x2 flujos espaciales (2x2:2)** en todas sus bandas de operación, siempre que soporten un ancho de canal (Channel Bonding) de hasta **320 MHz** y modulación **4096-QAM**. **Requisito Común:** Todos los equipos, independientemente de la opción elegida, deberán permitir la agregación de canales (Channel Bonding) de **al menos 80 MHz** en la banda de 5 GHz.

6.95.	IEEE 802.11ax beamforming o superior (Wi-Fi 6/6E y, cuando aplique, Wi-Fi 7), manteniendo interoperabilidad y desempeño en entornos densos.
6.96.	Los puntos de acceso deben permitir configuración de mínimo 8 SSIDs por access point gestionado de forma centralizada e integración con políticas de segmentación VLAN para redes corporativas, visitantes y dispositivos IoT y BLE.
6.97.	Disponer de una potencia de transmisión de por lo menos 18 dBm para 2.4GHz, 18 dBm para 5GHz y 18dBm para 6GHz
6.98.	La cantidad de equipos es la indicada en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".
	ACCESS POINT OUTDOOR
6.99.	Las características técnicas deben ser las misma de los **ACCESS POINT – AP** salvo las que se especifiquen a continuación.
6.100.	MU-MIMO multiusuario (enlace ascendente y descendente).
6.101.	Disponer de una potencia de transmisión de por lo menos 20 dBm para 2.4GHz, 20 dBm para 5GHz y 20 dBm para 6GHz.
6.102.	Las antenas pueden ser internas o externas cumpliendo con la ganancia mínima mencionada. Deben ser modelos resistentes a condiciones climáticas externas.
6.103.	Contar con un puerto ethernet: 1(2.5/5/10 Gbps)
6.104.	Los componentes de red deben soportar la instalación en ambientes adversos, su cantidad es la indicada en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO".
7	**DISPONIBILIDAD DEL SERVICIO**
7.1.	Para el servicio de Internet ofrecido, el contratista debe garantizar mínimo el noventa y nueve punto noventa y cinco por ciento (99.95 %) de disponibilidad del ancho de banda contratado. Por cada hora acumulada o constante que el sistema quede fuera de servicio (servicio de internet), el contratista deberá adicionar el equivalente a cinco (05) días de servicio al establecido en el contrato. Para el servicio de WIFI, ofrecido por el operador del servicio se debe garantizar el **99.6%** de funcionamiento de los Ap´s solicitados en el anexo "LUGARES Y CANTIDADES PRESTACIÓN SERVICIO". Cláusula: Por cada hora acumulada o constante que un AP este por fuera, el contratista deberá adicionar dos (02) días de servicio por cada AP que se encuentre fuera de servicio. El tiempo máximo para recuperación en caso de falla será de 4 horas en ciudades principales y 10 horas en ciudades intermedias en horarios hábiles. **No se computarán como indisponibilidad, para efectos de la adición de días de servicio de que trata el presente numeral:** **a) Las ventanas de mantenimiento preventivo programado, siempre que estas hayan sido previamente informadas y aprobadas por el supervisor del contrato, y se ejecuten dentro de los horarios y condiciones autorizadas.** **b) Las indisponibilidades originadas en causas no imputables al contratista, tales como fuerza mayor, caso fortuito o hecho exclusivo de un tercero, debidamente acreditadas por el contratista y validadas por el supervisor del contrato.** **En los eventos señalados en los literales a) y b), el tiempo de indisponibilidad correspondiente no será tenido en cuenta para el cómputo de las horas fuera de servicio ni para la adición de días de servicio establecida en el presente numeral, sin perjuicio de la obligación del contratista de reportar, documentar y sustentar oportunamente dichas causas ante el supervisor del contrato.** Cualquier indisponibilidad que se cause durante el transcurso del mes y durante la presentación del servicio contratado, distinta a las señaladas en los literales a) y b), podrá ser utilizado para el traslado o adquisición de nuevos AP's e infraestructura que sean requeridos durante la ejecución del contrato, sin generar costos adicionales para la Policía Nacional.
7.2.	El contratista deberá suministrar las herramientas necesarias para el monitoreo independiente del ancho de banda y del servicio de WiFi de cada una de las soluciones instaladas en las unidades de Policía, garantizando acceso para verificación por parte de la Policía Nacional (tableros, históricos y exportación de evidencias).

7.3.	Si el contratista requiere para dar continuidad a la prestación del servicio, implementar algún hardware y/o software, este deberá estar debidamente licenciado y autorizado para ser utilizado por la Policía Nacional. Se requiere que una vez sea instalado, se entregue a la Oficina de Tecnología de la información y las comunicaciones el original o copia autenticada de la licencia. En consecuencia, el contratista deberá garantizar la legalidad y originalidad de todo el software que se instale en la solución y presentará las licencias y certificados que lo soporten, sin generar costo alguno a la Policía Nacional. En cumplimiento a lo establecido en el artículo 61 de la C.P. que encarga al estado la obligación de proteger la propiedad intelectual mediante las formalidades que establezca la ley y garantizar el respeto por los Derechos de Autor y la propiedad intelectual bajo lo consagrado en la Ley 23/1982, Ley 178/1994 y todas aquellas que la modifiquen, adicionen o deroguen, al igual que los lineamientos trazados en este aspecto por la UAE Dirección Nacional de Derecho Autor y la Superintendencia de Industria y Comercio.
7.4.	El contratista deberá mantener durante la vigencia del contrato, un stock mínimo de diez (10) AP "access point" interiores (con todos sus accesorios) y cinco (05) AP exteriores (con todos sus accesorios).
7.5.	El contratista deberá garantizar el correcto funcionamiento de los enlaces, la plataforma de gestión y los equipos asociados desde el inicio y durante toda la vigencia, incluyendo soporte correctivo, reposición y estabilización cuando aplique.
7.6.	Se garantizará que todos los elementos de hardware y software instalados mantengan la funcionalidad con la que actualmente opera la POLICÍA NACIONAL, a partir del inicio del contrato y durante la vigencia del mismo.
7.7.	El contratista debe suministrar todas las herramientas necesarias de hardware y software para garantizar a la Policía Nacional la coadministración independiente de la solución integral de servicio de internet y WLAN. Ya que la administración de la seguridad perimetral estará bajo el cargo de los Administradores Red de Datos y Comunicaciones Unificadas del Grupo GUDAS de la Oficina de Tecnologías de la Información y las Comunicaciones.
7.8.	Los logs de todas las herramientas de la solución deberán permanecer en línea (disponibles para consulta) mínimo un (01) año; luego del año se deberán entregar en medio magnético al Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos de la Oficina de Tecnologías de la Información y las Comunicaciones, de igual forma el reporteador de la solución deberá soportar mínimo 200Gb de logs día con un crecimiento del 20% durante el término de vigencia del futuro contrato.
8	**SERVICIOS INCLUIDOS EN LA PRESTACIÓN DEL INTERNET**
8.1.	El contratista deberá suministrar, una capacidad de mínimo 210 direcciones IPv4 públicas para la Policía Nacional que se requieren para continuar con el servicio. Adicionalmente se debe continuar con la membresía ante LACNIC para el bloque de direcciones IPV6 con prefijo 40, el cual se encuentra a nombre de la Policía Nacional, durante el tiempo de ejecución del contrato.
9	**INFRAESTRUCTURA DE CONECTIVIDAD DEL ISP**
9.1.	Enrutamiento a nivel mundial en internet. El oferente deberá acreditar que su nodo de Internet cuenta con interconexión internacional redundante para enrutar tráfico hacia el backbone mundial, cumpliendo como mínimo con los siguientes criterios evaluables: a) Disponer de dos (02) salidas internacionales activas (rutas internacionales) con diversidad de ruta/operador, de forma que la falla de una salida no implique pérdida total de conectividad internacional. b) Mantener mecanismo de continuidad/conmutación (failover) o redundancia equivalente, que permita mantener la conectividad internacional ante contingencia de una de las salidas. c) Acreditar que dichas salidas no constituyen un único punto de falla (sin dependencia crítica de una sola ruta/enlace internacional sin mitigación). En este entendido, el oferente deberá **anexar obligatoriamente con la oferta una certificación** suscrita por representante autorizado del ISP/oferente y/o por el NOC del proveedor, donde conste explícitamente: • El número de salidas internacionales disponibles (mínimo 2) y su condición activa. • La diversidad de ruta/operador entre las salidas (sin necesidad de revelar información sensible). • La existencia del esquema de respaldo/conmutación (failover) o redundancia equivalente.

9.2.	El contratista debe contar con un sistema de respaldo de canal internacional con el ánimo de proporcionar la disponibilidad requerida en el ítem 7.1, debe tener como mínimo dos (02) salidas internacionales.
9.3.	El oferente deberá acreditar que no depende de otro operador para suministrar, administrar y monitorear integralmente el tramo de llegada a la Policía Nacional, entendido como: desde las instalaciones de la Policía Nacional (CPE/puerto de entrega) hasta el nodo/POP principal del ISP en Colombia incluyendo última milla, transporte/backhaul y monitoreo/NOC de ese tramo. El oferente deberá **anexar obligatoriamente con la oferta una certificación** suscrita por representante autorizado del ISP/oferente y/o su NOC donde conste explícitamente: a) Que el tramo de llegada es decir última milla + transporte/backhaul hasta el POP del ISP, es provisto, administrado y monitoreado directamente por el oferente, sin operación delegada en un tercero para esas funciones. b) Que el oferente cuenta con capacidad de monitoreo y gestión (NOC) sobre dicho tramo y que es el único responsable del diagnóstico, atención y restablecimiento ante fallas en ese segmento.
9.4.	**El oferente junto con la oferta deberá entregar las siguientes certificaciones vigentes:** • **Registro único de TIC emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones.** • **Asociación al NAP Colombia**
10	**SOPORTE TÉCNICO**
10.1.	El contratista deberá suministrar el servicio de Mesa de Ayuda con disponibilidad las veinticuatro (24) horas al día, siete (07) días a la semana, durante el plazo de ejecución del contrato, con las siguientes características: – Una línea de soporte para que la Policía Nacional pueda reportar inconvenientes o incidentes con la solución. – La mesa de ayuda deberá contar una herramienta para el seguimiento y control de los requerimientos reportados. – El soporte lo realizará profesionales con una experiencia mínima de dos (02) años en el campo de las telecomunicaciones e internet, con el fin de proporcionar una respuesta ágil y concisa a cualquier inquietud que se pueda presentar.
10.2.	Durante la ejecución del contrato se debe realizar un (01) mantenimiento preventivo por año a los equipos instalados, el cual debe incluir como mínimo: – Verificación del funcionamiento de los equipos suministrados. – Limpieza interna y externa, verificación de voltaje y revisión de conexiones. – Organización del cableado y elementos instalados. – Encendido de los equipos y funcionamiento de los mismos. – Actualización del software de monitoreo a las últimas versiones. – Entrega y firma del reporte del mantenimiento realizado.
10.3.	El contratista deberá entregar mensualmente reporte detallado de las indisponibilidades del servicio (descripción de la falla), fallas presentadas durante el mes y durante la vigencia del contrato.
10.4.	Para el servicio de soporte y mantenimiento de la plataforma de seguridad: El contratista deberá garantizar soporte correctivo remoto o en sitio cuando así se requiera con un esquema de atención 7x24, durante la vigencia del contrato. El contratista deberá realizar mínimo dos mantenimientos preventivos anuales durante el desarrollo del contrato. Las actividades mínimas que se realizarán corresponden a: • Revisión del correcto funcionamiento de la plataforma. • Aplicación de actualizaciones de versión o fixes o features, en caso de ser necesario y estar disponibles. • Revisión de logs de eventos y conexiones de tipo general, con el fin de detectar errores no reportados. • Revisión general de conexiones. • Copias de seguridad de las configuraciones. • Recomendar soluciones temporales y definitivas para errores identificados y notificados a los fabricantes.

	Para la prestación del servicio el contratista deberá disponer de una línea de atención telefónica que preste soporte técnico escalado a ingenieros de soporte certificados por el fabricante en el uso del producto, la configuración, el diagnóstico y la solución de problemas. El tiempo de respuesta telefónico será de máximo una hora. El tiempo de atención en sitio será en un máximo de tres horas.
11	**REQUERIMIENTOS DE COMPATIBILIDAD DE IPV6**
11.1.	Todo el hardware de TIC necesario para la prestación del servicio objeto de esta contratación debe funcionar adecuadamente con los protocolos IPv4 e IPv6, similar comportamiento se debe proporcionar para ambos protocolos de entrada, salida y/o el rendimiento de flujo de datos de rendimiento y la transmisión y el procesamiento de paquetes. Debe permitir compatibilidad de cualquier software que se comunica a través del protocolo IP con ambas versiones del protocolo (IPv4 e IPv6) a través de la solución contratada y la diferencia no debe ser perceptible para los usuarios. Los equipos capa 2 y capa 3 a implementar necesarios para la prestación del servicio objeto de la contratación, deben contar con el IPv6 Ready Logo o cumplir con las RFC que se enumeran a continuación: **Requerimientos para equipo "enterprise/ISP grade "Layer 2 switch** • IPv6 Basic specification [RFC2460] • MLDv2 snooping [RFC4541] • DHCPv6 filtering [RFC3315] • Router Advertisement (RA) filtering [RFC4862] • Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861] • Neighbor Unreachability Detection [NUD, RFC4861] filtering • Duplicate Address Detection [DAD, RFC4429] snooping y filtering.11 **Requerimientos para equipo "router or Layer 3 switch"** • IPv6 Basic specification [RFC2460] • IPv6 Addressing Architecture [RFC4291] • Default Address Selection [RFC3484] • Unique Local IPv6 Unicast Addresses (ULA) [RFC4193] • ICMPv6 [RFC4443] • SLAAC [RFC4862] • Multicast Listener Discovery versión 2 [RFC3810] • Router-Alert option [RFC2711] • Path MTU Discovery [RFC1981] • Neighbor Discovery [RFC4861] • Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] • IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996]
11.2.	**Requerimientos para el soporte IPv6 en software** Todo el software necesario para la implementación del servicio debe soportar IPv4 e IPv6 y ser capaz de comunicarse sobre redes sólo IPv4, sólo IPv6 y doble pila. Si el software incluye parámetros de red en su configuración de servidor local o remoto este debe además permitir la configuración de parámetros en IPv6.
11.3.	**Declaración de competencia en IPv6** Es necesario que el contratista declare sus competencias técnicas en IPv6, igualmente las de sus integradores, administradores y funcionarios de soporte, indicando el conocimiento y experiencia en IPv6, asegurando una apropiada instalación e integración de IPv6 en los ambientes TICS necesarios para la prestación del servicio. La declaración por parte del contratista bajo juramento de ley debe indicar: • Que tiene suficiente número de empleados para cumplir con los servicios ofertados. • Que estos empleados han sido entrenados profesionalmente para su trabajo de diseño, integración, construcción, administración y soporte del equipamiento TIC necesario para la implementación del servicio, en ambientes IPv4 e IPv6; • Que la calidad de los servicios ofertados cumple todos los requerimientos definidos en los documentos de la contratación y que estos requerimientos aplican tanto para IPv4 como para IPv6.

12	DOCUMENTACIÓN
12.1.	El contratista deberá entregar en medio digital (incluyendo esquemas, topologías, gráficas y texto) y separada por capítulos independientes una documentación total y actualizada de los equipos activos instalados: Un inventario de cada equipo tanto del hardware como del software que incluya entre otras cosas: tipo de elemento, Nro. de parte, versión de software, interfaces de red, configuración del enrutamiento, etc. Esta documentación debe haberse recibido a entera satisfacción por la Policía Nacional máximo a los treinta días (30) calendario después de haberse perfeccionado el contrato por las partes.
12.2.	El contratista debe entregar los planos de instalación donde queden ubicados los AP (con nombres/identificadores) y la topología de red de la solución implementada, en medio digital, garantizando que la información sea utilizable para auditoría, soporte y expansión.
12.3.	PRECIARIO: en la reunión del acta de inicio del contrato, el contratista deberá entregar al supervisor, un anexo que contenga el valor de los AP´s disgregado por departamento en el cual se encuentren la totalidad de los servicios a contratar (servicio de internet, seguridad, cableado de datos y eléctrico, soporte), con la finalidad de habilitar solicitudes futuras; estos valores deberán mantenerse durante la ejecución del contrato, conforme a las condiciones contractuales pactadas para todos los servicios solicitados.
12.4.	El oferente deberá entregar la ficha técnica de los equipos ofertados para la solución: 1. Router (Principal, Sedes) 2. UTM (Unified Threat Management) 3. Equipo Módulo de Estadísticas vía web 4. WAF (Web Aplication Firewall) 5. Equipo para la Solución de balanceo de carga 6. Equipo para el Servicio de Mitigación de Ataques de denegación de servicios distribuidos (DDoS por sus Siglas en Ingles) en sitio. 7. Switches de Acceso 8. Switches de Distribución 9. Switches de Core 10. Controladora de Access point 11. Access Point INDOOR 12. Access Point OUTDOOR
13	**GENERALIDADES**
13.1.	Todos los equipos activos, dispositivos de comunicación, accesorios, cables, patch cord, fibra óptica y demás elementos de hardware y de software necesarios en la instalación de cada servicio contratado, deben ser suministrados por el contratista sin generar costos adicionales a la Policía Nacional.
13.2.	El año de fabricación de los equipos suministrados por el contratista para la ejecución del presente contrato deberán ser igual o superior al **2024, de igual manera no deben estar declarados en fin de vida (EOL), ni con fin de soporte (EOS), para garantizar tecnología actual y soporte durante la vigencia del contrato.**
13.3.	El contratista deberá garantizar que los productos cuentan con soporte oficial durante la vigencia del presente contrato. En caso de que los elementos entren a su fin de ciclo de vida (End of Life -EOL) y/o fin de soporte (End of Support - EOS) deberán ser cambiados sin costo adicional para la institución por productos con características iguales o superiores a las exigidas en la ficha técnica.
13.4.	El contratista deberá garantizar que todos los dispositivos a instalar sean de última tecnología, no remanufacturados, con soporte vigente directamente con el fabricante durante la vigencia del contrato. El contratista para poder realizar la instalación de un equipo deberá entregar al supervisor del contrato la certificación de soporte vigente con el fabricante durante la vigencia del contrato.
13.5.	Los equipos suministrados por el contratista (switch de acceso, switch de distribución y switch core) deben ser del mismo fabricante, garantizando compatibilidades y óptimo funcionamiento con las controladoras y los Access Point.
13.6.	El contratista debe garantizar a la entidad la legitimidad de las licencias, entregando certificación de autenticidad, una vez se adjudique el contrato. Lo anterior, en cumplimiento a la circular conjunta 004 de 2006, emitida por la Dirección Nacional de Derechos de Autor y la Procuraduría General de la Nación. Las licencias deberán permitir upgrades de versión (mayores y menores), parches de seguridad y fixes sin costo adicional durante la vigencia.
13.7.	La Policía Nacional cuenta, dentro del Grupo de Comunicaciones Unificadas de la Oficina de Tecnologías de la Información y las Comunicaciones, con personal especializado que ostenta el cargo de ADMINISTRADOR RED DE DATOS Y COMUNICACIONES UNIFICADAS, quienes son los responsables de liderar, definir, administrar y salvaguardar la arquitectura, operación y evolución de la red institucional.

	En consecuencia, el Modelo de Gobierno dispuesto por el contratista deberá actuar en estricta alineación con los lineamientos técnicos, arquitectónicos, operativos y de seguridad definidos por los ADMINISTRADORES RED DE DATOS Y COMUNICACIONES UNIFICADAS, quienes ejercerán la autoridad técnica institucional sobre los servicios contratados. El personal de gobierno del contratista deberá acatar las directrices, procedimientos, estándares, validaciones y decisiones técnicas impartidas por dichos administradores, en lo relacionado con diseño de red, configuraciones, cambios, ampliaciones de capacidad, administración, monitoreo, seguridad, continuidad y optimización del servicio. Lo anterior, sin perjuicio de las responsabilidades contractuales del contratista, y en concordancia con el principio de que la gobernanza y control técnico de la red de datos y comunicaciones unificadas de la Policía Nacional es indelegable y permanece bajo la responsabilidad exclusiva de la Institución. Nota: En ningún caso el personal del contratista podrá implementar cambios, modificaciones, ampliaciones, reconfiguraciones o decisiones técnicas sobre la red institucional sin la validación, aprobación o instrucción expresa de los ADMINISTRADORES RED DE DATOS Y COMUNICACIONES UNIFICADAS de la Policía Nacional.
14	**CAPACITACIÓN**
14.1.	La capacitación se debe realizar con equipos de las mismas características técnicas de los utilizados para la prestación del servicio contratado, debe abarcar la instalación, configuración, administración, soporte y resolución de problemas de los distintos medios de hardware y software, el instructor deberá estar certificado y autorizado por el fabricante para dictar la capacitación y el pensum se debe desarrollar por el lapso de tiempo requerido por el fabricante de cada uno de los dispositivos, abarcando horas teóricas y horas de práctica, con el fin de que sea otorgada la respectiva certificación de la capacitación, las fechas y horarios de capacitación deben ser aprobados por el Supervisor del contrato, mediante la presentación de los respectivos pensum académicos. Dichas capacitaciones se deben realizar en horarios separados, de manera presencial en las instalaciones de los fabricantes de los equipos utilizados para la prestación del servicio o en las instalaciones de las instituciones debidamente acreditadas para dictar las capacitaciones y emitir las respectivas certificaciones. Cada una de las capacitaciones debe estar dirigida a seis (06) funcionarios de la Policía Nacional, encargados de la administración de la red institucional, del Grupo de Comunicaciones Unificadas, con el cargo de "Administrador de Red de Datos y Comunicaciones Unificadas" así: El contratista deberá brindar sin costo adicional para la Policía Nacional, la capacitación especializada y certificada sobre cada uno de los equipos a instalar para la prestación del servicio requerido en este proceso y como mínimo los temarios que se muestran continuación: **- EQUIPO ACTIVO ROUTER Y SWITCH** - Arquitectura y puesta en marcha - Conmutación L2 - Enrutamiento L3 - Servicios de red - Calidad de servicio (QoS) - Seguridad en switching/routing - Operación y administración - Monitoreo y resolución de problemas - Buenas prácticas de documentación **- CONTROLADORA DE LA SOLUCIÓN WLAN** - Arquitectura WLAN gestionada - Configuración de WLAN/SSIDs y políticas - Seguridad WLAN - Radiofrecuencia (RF) y optimización - Roaming y movilidad - Gestión, monitoreo y analítica - Integración con servicios de red - Operación y troubleshooting WLAN

- Actualizaciones y continuidad
- Diseño y análisis de cobertura WIFI

- ACCESS POINT

- Instalación y puesta en servicio
- Modos de operación
- RF práctico
- Rendimiento y experiencia de usuario
- Seguridad en AP
- Mantenimiento y soporte
- Troubleshooting de campo

- IPV6

- Fundamentos del direccionamiento IPv6 Subnetting y Summarizacion.
- Autoconfiguración y direcciones temporales
- Configuración de IPv6 en redes y servicios incluyendo direccionamiento, descubrimiento, autoconfiguración, DNS IPv6, ruteo IPv6 y DHCPV6
- Mecanismos de transición a IPV6
- Introducción a la seguridad IPv6.
- Vulnerabilidades de seguridad de IPv6.
- Herramientas de seguridad para IPv6.
- Seguridad IPv6 en dispositivos de red.
- Solución de problemas de IPv6.
- Y otros que sean necesarios para su correcto funcionamiento.

- EQUIPO UTM (UNIFIED THREAT MANAGEMENT)

- Arquitectura y componentes del UTM
- Puesta en marcha y operación básica
- Políticas de firewall de nueva generación (NGFW)
- Control de navegación y visibilidad por usuario
- Web Gateway / filtrado por categorías
- Reportería y tableros operativos
- Identidades e integración con directorio
- Operación en IPv4 e IPv6
- Monitoreo, soporte y troubleshooting

- EQUIPO DE ESTADÍSTICAS VÍA WEB

- Arquitectura y alcance del módulo
- Acceso seguro y operación por HTTPS
- Utilización del canal – lectura e interpretación
- Sitios web visitados – explotación del "top 10"
- Segmentación de tráfico requerida
- Indicadores de calidad (última milla)
- Operación, soporte y troubleshooting del módulo

Por otro lado, se requiere la transferencia de conocimiento para seis (06) funcionarios de la Policía Nacional, encargados de la administración de la red institucional, del Grupo de Comunicaciones Unificadas, con el cargo de "Administrador de Red de Datos y Comunicaciones Unificadas" y dos (02) funcionarios del Grupo Seguridad de la Información y respuesta a Incidentes Informáticos, de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional y abarcar como mínimo instalación, configuración, administración, soporte y resolución de problemas. El instructor deberá estar certificado y autorizado por el fabricante del equipo ofertado para impartir la capacitación; el pensum incluirá componente teórico y práctico y se entregarán materiales, evidencias de asistencia y constancia/certificación de finalización, así:

	- EQUIPO WAF (WEB APLICATION FIREWALL) **- EQUIPO PARA BALANCEO DE CARGA** **- DISPOSITIVO DE MITIGACIÓN DE ATAQUES DDOS** Adicionalmente, los funcionarios de la Policía Nacional deberán participar de forma activa en la instalación, configuración, verificación y afinamiento de los equipos necesarios para la prestación del servicio por parte del contratista; la capacitación debe ponerse en práctica por parte de los ocho (8) funcionarios de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, quienes serán instruidos por el personal de la empresa contratista durante la implementación y configuración de todos los elementos de Hardware y Software que se requieran para la prestación del servicio, incluyendo la topología de red establecida por el contratista. Para ello se realizará una transferencia de conocimiento en la cual se determinen y expliquen de forma clara las características técnicas del servicio implementado en la institución, a través de mínimo cuarenta (40) horas adicionales de capacitación, la cual se realizará en las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, dentro del plazo de ejecución del contrato.

Patrullero **ADICXON QUINTO SANCHEZ**
Estructurador estudio previo

Intendente **LUIS FERNANDO RIVERA BARRAGÁN**
Estructurador estudio previo

Mayor **JHON ALEXANDER MENDEZ MENDOZA**
Jefe Grupo Comunicaciones Unificadas (E)