MINISTERIO DE DEFENSA NACIONAL

POLICÍA NACIONAL

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

FORMATO No. 2

<table>
<tr><th colspan="2">FORMATO PARA SOLICITAR COTIZACIONES</th></tr>
<tr><td>ADVERTENCIA</td><td>Se indica que la cotización requerida servirá de base para la elaboración de un estudio de mercado y, por tanto, no constituye en sí misma una oferta y consecuentemente NO obliga a las partes.</td></tr>
<tr><td>OBJETO</td><td>“ADQUISICIÓN DE SERVICIOS DE CONECTIVIDAD Y CANALES DEDICADOS DE DATOS PARA GARANTIZAR LA OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS DE LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL”.
<table>
<tr><th>CLASIFICACIÓN UNSPSC</th><th>SEGMENTO</th><th>FAMILIA</th><th>CLASE</th><th>PRODUCTO</th></tr>
<tr><td>83112304</td><td>83000000
Servicios públicos y servicios relacionados con el sector público.</td><td>83110000
Servicio de medios de telecomunicaciones</td><td>83112300
Servicio de telecomunicaciones por fibra</td><td>83112304
servicio de trasmisión óptica.</td></tr>
</table></td></tr>
<tr><td>VALIDEZ DE LA COTIZACIÓN</td><td>La cotización debe tener una validez mínima de 90 días calendario.</td></tr>
<tr><td>ESPECIFICACIONES TÉCNICAS</td><td>
<table>
<tr><th colspan="4">LOTE 1: ADQUISICIÓN DE SERVICIO DE CANALES DEDICADO MPLS Y DE INTERNET PARA LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL.</th></tr>
<tr><th>ÍTEM</th><th colspan="2">DESCRIPCIÓN</th><th>OFERTA/NO OFERTA</th></tr>
<tr><td rowspan="7">1.</td><td colspan="2">ADQUISICIÓN DE SERVICIO DE CANALES DEDICADOS MPLS Y DE INTERNET PARA LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL.</td><td rowspan="7"></td></tr>
<tr><td>ÍTEM</td><td>DESCRIPCIÓN / CANTIDAD</td></tr>
<tr><td>1</td><td>CANAL DEDICADO INTERNET DE 100 Mbps — 1</td></tr>
<tr><td>2</td><td>CANAL PRINCIPAL DEDICADO MPLS DE 500 Mbps — 1</td></tr>
<tr><td>3</td><td>CANAL DISASTER RECOVERY (DR) DEDICADO MPLS DE 250 Mbps — 1</td></tr>
<tr><td>4</td><td>CANAL DEDICADO MPLS DE 100 Mbps – SACOM2-NEIVA. — 1</td></tr>
<tr><td>5</td><td>CANAL DEDICADO MPLS DE 100 Mbps – SACOM3-PEREIRA. — 1</td></tr>
<tr><td>6</td><td>CANAL DEDICADO MPLS DE 100 Mbps – SACOM4-POPAYÁN. — 1</td></tr>
</table></td></tr>
</table>

			7	CANAL DEDICADO MPLS DE 100 Mbps – SACOM5-FLORIDABLANCA.	1		
			8	CANAL DEDICADO MPLS DE 100 Mbps – SACOM6-MEDELLÍN.	1		
			9	CANAL DEDICADO MPLS DE 100 Mbps – SACOM7-VILLAVICENCIO.	1		
			10	CANAL DEDICADO MPLS DE 100 Mbps – SACOM8-BARRANQUILLA.	1		
			11	CANAL DEDICADO MPLS DE 100 Mbps – SACOM MECAL.	1		
			El contratista deberá garantizar la totalidad de la cobertura y contar con la infraestructura necesaria a nivel nacional y local que permita la conexión y comunicación de las diferentes sedes descritas, suministrando para cada uno de los sitios relacionados a continuación un canal dedicado de Internet y MPLS soportados en fibra óptica, de acuerdo con las características y el ancho de banda solicitado.				
			DATA CENTER - RACOI	CARRERA 62 # 19-04 INT 1 ZONA INDUSTRIAL-PUENTE ARANDA BOGOTÁ-CUNDINAMARCA. CANAL DE INTERNET DEDICADO.			
			DATA CENTER - RACOI	CARRERA 62 # 19-04 INT 1 ZONA INDUSTRIAL-PUENTE ARANDA BOGOTÁ-CUNDINAMARCA. CANAL PRINCIPAL MPLS.			
			DATA CENTER - DIJIN	AV. EL DORADO # 75 - 25 MODELIA BOGOTÁ-CUNDINAMARCA. DISASTER RECOVERY (DR). PUNTO MULTI PUNTO MPLS.			
			SACOM 2	CALLE 21 SUR #6-235-ZONA INDUSTRIAL-REGIONAL DE POLICIA Nº2. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM 3	AV. DE LAS AMERICAS #46-35 - COMANDO DE POLICIA METROPOLITANA DE PEREIRA. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM 4	AV. PANAMERICANA # 1N-75 BARRIO VILLA PAULA-COMPLEJO POLICÍA IJ DIEGO GUERRERO POPAYÁN-CAUCA. CANAL PUNTO MULTI PUNTO MPLS.			

			SACOM 5	TRANSVERSAL 203 # 27A-01 VÍA RUITOQUE BAJO KILOMETRO 1-COMPLEJO POLICÍA NACIONAL FUERTE SUR FLORIDABLANCA-SANTANDER. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM 6	CALLE72 # 64-70 BARRIO CARIBE-SIJIN MEVAL MEDELLÍN-ANTIOQUIA. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM 7	CALLE 44 # 35C-02 - EL TRIUNFO-COMANDO POLICIA META. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM 8	CALLE 74 # 38-13 - LAS DELICIAS-COMPLEJO REGIONAL DE CRIMINALISTICA Nº8. CANAL PUNTO MULTI PUNTO MPLS.			
			SACOM MECAL	CALLE 21 # 1N-65 - BARRIO PILOTO-COMANDO POLICIA METROPOLITANA DE CALI. CANAL PUNTO MULTI PUNTO MPLS.			
		1.1	El contratista deberá suministrar los canales dedicados, los cuales deberán contar con velocidad simétrica (subida y bajada), de acuerdo con las características del ancho de banda requerido.				
		1.2	**Redistribución dinámica e incremento del ancho de banda MPLS.** El contratista deberá contar con la capacidad técnica, logística y de personal para gestionar el ancho de banda de los enlaces MPLS sin costo adicional para la Policía Nacional y dentro del límite total contratado. Esta gestión deberá permitir la redistribución flexible y dinámica de la capacidad entre las distintas sedes, incrementando el ancho de banda en un canal mediante la disminución proporcional en otros, sin afectar la disponibilidad del servicio, así como la realización de incrementos por necesidades del servicio a solicitud del supervisor del contrato, garantizando que todo ajuste formalmente solicitado sea aplicado en un plazo no mayor a 24 horas conforme a las políticas de gestión de red acordadas.				
		1.3	El contratista deberá proporcionar el 100% de la capacidad solicitada para cada uno de los canales contratados en las diferentes sedes descritas.				
		1.4	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.				
		1.5	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. 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.				

		1.6	La solución debe contar 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 solicitados para las sedes descritas.			
		1.7	El contratista deberá suministrar los canales dedicados por un tiempo de dos (2) años, brindando garantía y soporte sobre el servicio durante el mismo periodo.			
		1.8	El contratista deberá garantizar la continuidad del servicio desde la adjudicación del contrato, hasta tanto se instale la totalidad de los servicios con los que actualmente cuenta la institución y los nuevos servicios requeridos en las sedes descritas, sin generar costos adicionales a la Policía Nacional.			
		1.9	**VISITA A INSTALACIONES** La Dirección de Investigación Criminal e INTERPOL, con el fin de facilitar a los oferentes el conocimiento de los aspectos técnicos y finalidad de lo que se pretende adquirir por parte de la entidad, programará una visita a los diferentes sitios anteriormente nombrados, en coordinación con el Jefe de Recepción de Análisis de Comunicaciones Interceptadas, para verificar las condiciones técnicas establecidas en el presente proceso, en coordinación con el estructurador del estudio previo y el supervisor del contrato para verificar las mismas. La fecha y hora de la visita se establecerán en la Convocatoria Pública, pliego definitivo, la cual será publicada en la página de Colombia Compra Eficiente www.colombiacompra.gov.co, una vez se efectúe la apertura del proceso. Se aclara que dicha visita será de carácter informativo y **NO ES REQUISITO HABILITANTE O DE OBLIGATORIO CUMPLIMIENTO, así mismo, se informará cambios en el cronograma por situaciones de orden público que impidan la realización de la actividad.** **Nota:** La no asistencia a la visita a la Dirección de Investigación Criminal e INTERPOL no exonera al proponente (futuro contratista) de su responsabilidad en la ejecución del contrato y, por tanto, no podrá invocar este incidente como excusa para efectuar posteriores reclamaciones o no dar cumplimiento al contrato que firmen las partes. **Justificación:** La visita al sitio donde se realizará la *"ADQUISICIÓN DE SERVICIO DE CANALES DEDICADOS MPLS Y CANAL DE INTERNET DEDICADO PARA PARA LA DEPENDENCIA DE RECEPCIÓN Y ANÁLISIS DE COMUNICACIONES INTERCEPTADAS".* Le permite al oferente conocer de primera mano los lugares exactos donde se desarrollará dicha actividad, relacionadas en este proceso. La Dirección de Investigación Criminal e INTERPOL, podrá reprogramar o cancelar la visita por motivos de seguridad.			
		1.10	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.			
		1.11	El contratista deberá marcar todo el hardware y cableado que instale para cada servicio contratado con el fin de facilitar su identificación y ubicación.			

		1.12	El contratista deberá garantizar la configuración de los Router a instalar, en el Data Center de las instalaciones de RACOI, con todos los protocolos y enrutamientos necesarios que permitan el tráfico de todos los segmentos de red establecidos en cada uno de los lugares descritos. **Nota:** Dicha configuración deberá permitir; lectura/escritura controlada, respaldo de configuraciones, visibilidad de licencias y capacidades reales.			
		1.13	El contratista deberá garantizar la configuración de los router a instalar, con todos los segmentos de red establecidos en cada uno de los lugares descritos. **Nota:** Dicha configuración deberá permitir; lectura/escritura controlada, respaldo de configuraciones, visibilidad de licencias y capacidades reales.			
		1.14	El contratista deberá suministrar un software que permita visualizar en tiempo real, el estado de los servicios contratados, donde se evidencie: • Estado actual de los servicios. • Diagnóstico de tráfico. • Alarmas de fallas en los servicios. • Alarmas de fallas en los componentes de los servicios. • Generación de reportes (diarios, semanales, mensuales y anuales). • Accesos con roles diferenciados. Posibilidad de auditoría técnica. **Nota:** El acceso suministrado al software en mención deberá permitir auditoría, trazabilidad de cambios y consulta histórica de configuraciones.			
		1.15	Para los eventos de fallas masivas o degradación de los canales, estos se deben reportar en forma INMEDIATA al supervisor del contrato mediante correo electrónico. Adicionalmente se deberá informar mediante correo electrónico, cuando se recupere el servicio, cuantificando el tiempo de duración de la falla.			
		1.16	El contratista deberá entregar al supervisor del contrato, usuario y contraseña del software requerido en el ítem 1.14, para verificar y descargar los eventos de falla que presenten en los servicios contratados.			
		1.17	El contratista deberá mantener el servicio continúo sin limitaciones funcionales durante las 24 horas del día, durante toda la vigencia del servicio.			
		1.18	El contratista debe entregar operando el canal dedicado sin superar los 15 días calendario una vez aprobadas las pólizas.			
		1.19	El contratista debe proporcionar los equipos de conectividad necesarios para suministrar el canal dedicado de Internet y/o MPLS, punto multi punto y que opere con normalidad.			
		1.20	El contratista debe proporcionar el equipo de conectividad tipo (router) que sea necesario para garantizar el acceso a la red principal del canal de internet dedicado una vez adjudicado el contrato.			
		1.21	La arquitectura de comunicaciones y conectividad debe estar totalmente independiente de la red de la Policía Nacional.			

		1.22	El contratista, suministrará los componentes necesarios de hardware y software que permitan la conectividad desde los nodos hacia los equipos ubicados en los sitios anteriormente informados para las respectivas instalaciones.			
		1.23	El contratista deberá garantizar la disponibilidad de los canales dedicados durante toda la totalidad de la vigencia del servicio.			
		1.24	Si durante el desarrollo del proyecto se encuentra que el contratista no incluyó elementos o documentación que no permita la normal prestación de servicio, deberá incluirlo, suministrarlo, instalarlo y ponerlo en funcionamiento sin costo adicional para la Policía Nacional. El hecho que se detecten errores u omisiones en estos términos de referencia, pliegos o especificaciones técnicas, no libera al contratista de ejecutar satisfactoriamente el objeto del contrato en las fechas estipuladas para su ejecución, incluyendo etapas de soporte y garantía.			
		1.25	El contratista deberá asumir todos los daños que puedan generar el mal ensamblaje o manipulación de cualquier elemento del espacio donde se estén realizando las instalaciones.			
		1.26	El contratista deberá disponer de mano de obra calificada, así como de los equipos necesarios para dar cumplimiento al objeto contractual.			
		1.27	El contratista se obliga a cumplir los tiempos y actividades plasmadas en los cronogramas del proyecto disponiendo de todos los medios y recursos para tal fin.			
		1.28	Todos los elementos requeridos para la puesta en operación del presente objeto contractual deben ser nuevos. No debe haber reutilización de ningún material.			
		1.29	Para las actividades de instalación de componentes del presente proyecto, no se pueden intervenir ni alterar elementos estructurales principales; el contratista deberá conservar las especificaciones y los diseños de los componentes estructurales y arquitectónicos.			
		1.30	En aras de prestar un correcto y adecuado servicio, el contratista suministrará el software que sea necesario debidamente licenciado por el tiempo requerido a nivel contractual.			
		1.31	Al momento que el contratista ingrese a las instalaciones para realizar la instalación del servicio, deberán tener un acompañante por parte de la Policía Nacional para el desplazamiento dentro de las instalaciones por temas de seguridad.			
		1.32	El contratista deberá implementar todos los controles necesarios para evitar fuga de información.			
		1.33	El contratista, deberá diligenciar el formato 1DT-FR-0016 "*Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros*".			
		2	**SEGURIDAD**			
		2.1	El contratista se compromete a cumplir los lineamientos establecidos bajo la resolución de seguridad de la información *"Resolución 04408 de 26122024 Manual SGSI de la Policía Nacional Por la cual se expide el manual del sistema de gestión de seguridad de la información para Policía Nacional".*			

		2.2	**CONFIDENCIALIDAD DE LA INFORMACIÓN:** En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato, y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el Formulario *"ACUERDO DE CONFIDENCIALIDAD"*.			
		2.3	Si la Policía Nacional, considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la entidad le solicite para este fin.			
		2.4	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física, Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, para lo cual deberá diligenciar el formulario *"SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO"* (SGSST).			
		2.5	El contratista y su personal deberá cumplir las políticas de seguridad de la información que se encuentra en el Manual del Sistema de Seguridad de la Información para la Policía Nacional y demás normas concordantes, el contratista y sus empelados deberán firmar los formatos de declaración de confidencialidad y compromiso con la seguridad de la información contratistas y terceros, lo anterior dando cumplimiento a la política de seguridad de información DIJIN.			
		2.6	El contratista que por el desempeño de sus funciones conozcan de métodos, procedimientos información, infraestructura, doctrina, medios, productos, entre otros que son de propiedad de origen o proceso de la Policía Nacional y en el ejercicio de sus actividades hayan visto, oído o comprendido están amparadas bajo la reserva legal, teniendo en cuenta los parámetros legales de la ley estatutaria 1581 del 2012 y la ley 1712 de 2014, en pro de las personas que son objeto de tratamiento como apoyo a la administración de la justicia en la lucha contra la impunidad. De igual manera se transfiere la reserva legal de la información teniendo en cuenta que es responsabilidad del funcionario solicitante garantizar, que la información que origina o procesa la Dirección de Investigación Criminal e INTERPOL, debe mantener el principio de segmentación a partir de la necesidad de saber y conocer estrictamente lo necesario para el desempeño de la función que le es propia, el acceso, uso y disposición final de la misma. Lo anterior teniendo en cuenta los parámetros establecidos en la ley 1581/2012 y Ley 1712/2014 que refiere a garantizar los derechos fundamentales, constitucionales y legales de los datos de las personas que son objeto de tratamiento y son almacenadas en nuestras bases de datos, enmarcadas en las actividades que realizan los funcionarios adscritos a la DIJIN en liderar la Investigación Criminal y apoyar la administración de la justicia.			
		2.7	El contratista se acogerá a lo dispuesto a través de la norma ISO 27001:2013 Sistema de Gestión de Seguridad de la Información, dando cumplimiento a todas las expectativas y requisitos de la norma.			
		2.8	El contratista está obligado a garantizar a la entidad la legitimidad de las licencias, salvaguardándola de cualquier responsabilidad por el uso del programa autorizado.			

		2.9	Firewall	El contratista deberá suministrar, instalar, configurar y dejar en funcionamiento en la sede principal un firewall físico con tecnología UTM o de próxima generación, destinado a la protección, administración y control del tráfico asociado al canales dedicados y de internet de 100 MBPS.			
				El firewall debe ser físico y debe prestar los servicios básicos de firewall, NAT, sin afectar el desempeño del canal.			
				El firewall debe ser mínimo un dispositivo con tecnología UTM.			
				El equipo deberá contar como mínimo con las siguientes condiciones: • Throughput general de 10 Gbps (10,000 Mbps) como mínimo. • Throughput por interfaz 1 Gbps (10/100/1000 Mbps) como mínimo. • Licenciamiento para tráfico cifrado de 6.5 Gbps IPsec VPN / 630			

				Mbps SSL Inspection como mínimo. • Chasis integrado. • Soportar protocolos de enrutamiento IPv4, IPv6, BGP, OSPF, RIP, VRF, VRRP y FortiGate HA como mínimo. • Soportar protocolo SNMP v1, v2c y v3 para la gestión de eventos como mínimo. • Soportar Protocolo de cifrado túnel VPN GRE, IPsec VPN y SSL VPN como mínimo. • Soportar Protocolo de cifrado IPSEC-AES256 como mínimo. • Control del tráfico entrante y saliente. • Control de calidad de servicio QoS. • Soporte con fabricante durante la duración del contrato. • Alta escalabilidad.			
				Marca y modelo: especificar.			
				VPN: el firewall debe permitir la configuración VPN para conexión segura con otras entidades y acceder a servicios y plataformas de consultas externos.			
				Instalación física: Carrera 62 # 19-04 Int 1 Zona Industrial-Puente			

				Aranda Bogotá-Cundinamarca.			
				Debe disponer de bloqueo de gusanos, troyanos, malware, spam, intrusiones, ataques de denegación de servicio (DoS) y otras amenazas.			
				Deberá permitir la inspección y control de protocolos como HTTP, HTTPS, FTP, SMTP y POP3, así como el control de aplicaciones y el filtrado de contenido web.			
				Deberá contar con gestión centralizada mediante interfaz web o API, consulta de registros, generación de alertas y actualización de firmas de seguridad.			
				El contratista deberá realizar un análisis inicial de la red, definir y configurar las políticas de seguridad, ejecutar pruebas de funcionamiento y realizar un análisis de vulnerabilidades posterior a la implementación. Los resultados deberán entregarse al supervisor en un informe técnico.			
				Disponer de una proporción de detección de SPAM de mínimo un 95%.			
				Las licencias, actualizaciones, soporte y servicios de seguridad requeridos para el correcto funcionamiento del firewall deberán permanecer vigentes durante los dos (2) años de ejecución contractual sin que se genere un costo adicional para la Policía Nacional.			
				Capacidad mínima para 200 usuarios.			

				El equipo deberá contar con un rendimiento de firewall mínimo de 10 Gbps, medido con tráfico bidireccional, sin degradación del servicio y certificado por el fabricante.			
				El equipo deberá contar con gestión centralizada mediante interfaz web o API.			
				Actualización: el contratista debe realizar las actualizaciones a que haya lugar durante el tiempo de servicio sin que se genere un costo adicional para la Policía Nacional.			
		3	**SOPORTE**				
		3.1	El contratista se compromete a obrar con diligencia ante problemas que se presenten con el servicio adquirido y para el restablecimiento del mismo en caso de ser necesario durante la totalidad de la vigencia del contrato.				
		3.2	El contratista informará de manera oportuna al supervisor del contrato la realización de ventanas de mantenimientos que afecten el servicio y su tiempo de duración durante la vigencia del contrato.				
		3.3	El contratista dispondrá de mínimo 02 medios de comunicación disponibles los 7 días de la semana y las 24 horas de día, a través de los cuales el supervisor del contrato le podrá escalar requerimientos de soporte durante la vigencia del servicio. Estos medios de contacto serán informados dentro de la documentación presentada al supervisor por parte del gerente del proyecto.				
		3.4	El contratista ante cualquier problema de disponibilidad del servicio del canal dedicado, efectuará las gestiones necesarias tan pronto tenga conocimiento de la novedad para que se logre el restablecimiento del servicio en el menor tiempo posible sin sobrepasar las 06 horas.				
		3.5	El contratista garantizará que el canal de datos ofertado, dispondrá por parte del proveedor del servicio de soporte y atención técnica especializada capaz de ayudar a resolver cualquier tipo de problema que pueda surgir.				
		3.6	Cuando el soporte por los medios de comunicación relacionados en el ítem 3.3 no sea suficientes para dar solución a los problemas presentados, el contratista debe proporcionar soporte presencial en las instalaciones de la dependencia Recepción y Análisis de Comunicaciones Interceptadas (RACOI), dentro de las 06 horas siguientes a la toma de contacto por medio de los canales de soporte establecidos. Los gastos que se generen producto de la asistencia en sitio serán asumidos por el contratista en su totalidad.				
		3.7	Los daños ocasionados en atención a la prestación de soporte del canal dedicado de acceso internet, serán asumidos por el contratista, quien deberá subsanarlos garantizando dejarlos en iguales o mejores condiciones de las que estaban, sin que se genere un costo adicional para la Policía Nacional.				

		3.8	Si un mismo equipo presentara problemas en su correcto funcionamiento o se haya reparado más de dos veces, este deberá ser remplazado por el contratista sin que se genere un costo adicional para la Policía Nacional durante toda la vigencia del servicio.			
		3.9	En caso de que uno de los equipos deba ser retirado por el contratista para ser reparado o cambiado por presentar inconvenientes técnicos, este será remplazado por uno de iguales o superiores características técnicas hasta tanto sea puesto nuevamente en funcionamiento.			
		4	**PERSONAL MÍNIMO DE TRABAJO**			
		4.1	El oferente deberá acreditar como mínimo uno (1) o dos (2) profesionales en Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con matrícula o tarjeta profesional vigente.			
		4.2	El profesional deberá contar con experiencia mínima de tres (3) años, contada a partir de la expedición de la matrícula o tarjeta profesional cuando corresponda, relacionada con redes de datos, canales dedicados, MPLS, fibra óptica o áreas afines.			
		4.3	El oferente deberá presentar copia de la hoja de vida, documento de identidad, título profesional, matrícula o tarjeta profesional vigente.			
		4.4	El profesional deberá acreditar formación o certificaciones relacionadas con seguridad de la información, redes de telecomunicaciones, diseño de soluciones de fibra óptica o administración de soluciones de seguridad perimetral.			
		4.5	El profesional administrará la conectividad y el firewall, garantizando su correcta configuración y soporte. Será responsable de atender incidentes, realizar pruebas técnicas, acompañar los mantenimientos programados y presentar los informes requeridos por la supervisión del contrato.			
		5	**DOCUMENTACIÓN**			
		5.1	El contratista suministrará certificación en la que se evidencie que el canal es dedicado de uso exclusivo sin reúsos, y de capacidades simétricas de subidas y bajadas.			
		5.2	El contratista suministrará esquema de conexión final de la infraestructura de red implementada, en la que de detalle cada uno de los componentes.			
		5.3	El contratista deberá entregar toda la documentación técnica de elementos y periféricos instalados, organizados en un diagrama de conexión.			
		5.4	El contratista se compromete a entregar los manuales, instaladores, guías de usuario y toda la información técnica en idioma español para su correcta configuración y uso, de ser necesario.			
		5.5	El contratista deberá entregar en la etapa de inicio el cronograma de ejecución y plan de trabajo, para previa aprobación del supervisor del contrato.			
		5.6	El contratista debe presentar los cronogramas de ejecución en diagrama de Gantt de Ms Project en físico y digital. Los cronogramas deben ser aprobados por la supervisión del contrato, el pago estará condicionado a la entrega y recibo a satisfacción del proyecto, sin exceder el tiempo de ejecución contractual.			
		5.7	El contratista suministrará documentación que permitía validar la adquisición del acceso al servicio de canal dedicado y sus características por un periodo de dos (02) años.			

		5.8	El oferente deberá adjuntar la ficha técnica oficial del firewall propuesto, en la cual se puedan verificar todas las características mínimas exigidas. No será obligatorio indicar una marca determinada, siempre que la solución cumpla o supere las especificaciones solicitadas.			
		5.9	El oferente deberá adjuntar las fichas técnicas de los routers, equipos de borde, módulos, interfaces y demás equipos relevantes que serán utilizados para la prestación del servicio.			
		6	**PRESENTACIÓN DE LA OFERTA**			
		6.1	El oferente, deberá presentar la siguiente documentación junto con la oferta: Carta firmada por el representante legal de la empresa oferente, dirigida a la Dirección de Investigación Criminal e INTERPOL, a través de la cual certifique los siguientes aspectos: • Certificación de los canales ofertados serán de acuerdo a las capacidades solicitadas para cada uno de los sitios durante 2 años. • Relación de los canales de comunicación disponibles para el reporte de incidentes con el servicio según la especificación del ítem 3.4. • Certificación en la que se evidencie que el canal es dedicado de uso exclusivo sin reúsos y de capacidades simétricas de subidas y bajadas. • Fichas técnicas que contengan las características técnicas de los equipos que serán instalados para el suministro del servicio de iguales o superiores especificaciones requeridas.			
		7	**GARANTÍA**			
		7.1	El contratista garantizará la disponibilidad del servicio los siete (07) días de la semana las veinticuatro (24) horas del día durante la vigencia del servicio. En caso de presentarse indisponibilidad del servicio, el contratista repondrá el tiempo, siendo adicionado a la fecha de finalización del contrato sin que se genere un costo adicional para la Policía Nacional.			
		7.2	El tiempo de la garantía será por dos (2) años contado a partir del recibo a conformidad.			
		7.3	El contratista deberá realizar todas las configuraciones necesarias para lograr el enrutamiento en todos los equipos de los canales de datos propios y contratados, garantizando el acceso de todos los segmentos de red a la red de datos de la Institución. Si para lograr la integración se requieren equipos adiciónales, estos deben ser aprovisionados por el contratista sin generar costos adicionales a la Policía Nacional.			
		8	**REPORTES**			

		8.1	El contratista deberá presentar al supervisor del contrato un informe mensual de la totalidad de los servicios contratados, que contenga como mínimo la siguiente información: estadística de consumo, capacidad, disponibilidad y monitoreo de servicios, pico máximo de consumo, análisis de consumo mayor al 70%; esta información se entregará en medio magnético.			
		8.2	El contratista deberá presentar al supervisor del contrato, reporte mensual detallado de las indisponibilidades de los servicios contratados durante el mes, esta información se entregará en medio magnético.			
		9	**DISPONIBILIDAD**			
		9.1	El contratista deberá garantizar una disponibilidad del (99.6 %) mensual, en los servicios contratados en todas las sedes descritas anteriormente. **Nota:** por cada hora de afectación a la disponibilidad en los servicios contratados, el contratista deberá adicionar la equivalencia a dos (02) días de servicio al establecido en el contrato. La indisponibilidad la establecerá el supervisor del contrato y el contratista, teniendo en cuenta lo reportado por el software de gestión solicitado y verificando las fallas atribuibles al contratista.			
		9.2	El valor de las indisponibilidades que se causen durante el trascurso del mes y durante la prestación del servicio contratado, podrán ser utilizadas para la ampliación de servicios contratados o para adquirir nuevos servicios de conectividad que sean requeridos durante la ejecución del contrato, previa coordinación con el supervisor del contrato.			
		9.3	De presentarse tres (03) indisponibilidades recurrentes en algunos de los sitios descritos en un periodo móvil de tres meses durante la vigencia del contrato, el contratista deberá realizar el cambio de tecnología o solución adecuada para la óptima prestación del servicio en dicho lugar, sin generar costos adicionales a la Policía Nacional. Para las ampliaciones de servicios contratados, se deberán realizar con un plazo máximo de quince (15) días calendario, una vez la solicitud sea aprobada por parte del supervisor sin generar costo adicional para la policía nacional. Se podrá solicitar prórroga para la ampliación de servicios contratados, presentando los respectivos soportes que indiquen fuerza mayor o caso fortuito, informando al supervisor del contrato, por lo menos cinco (05) días calendario antes de cumplirse la fecha límite. **Nota:** por cada hora de afectación a la disponibilidad en los servicios contratados, el contratista deberá adicionar la equivalencia a dos (02) días de servicio al establecido en el contrato. La indisponibilidad la establecerá el supervisor del contrato y el contratista, teniendo en cuenta lo reportado por el software de gestión solicitado y verificando las fallas atribuibles al contratista.”			
		10	**REQUERIMIENTOS DE MANTENIMIENTO**			
		10.1	Una vez inicie el contrato, el contratista deberá presentar al supervisor del contrato para su aprobación, un plan de mantenimiento preventivo de los servicios contratados, anexando cronograma detallando tanto fechas, como sedes a visitar.			

10.2	El contratista deberá realizar mantenimientos preventivos a todos los equipos de los servicios contratados, en periodicidad de ocho (08) meses durante la vigencia del contrato, garantizando el correcto funcionamiento y certificación de los servicios, donde mínimo deben realizar las siguientes actividades sin generar costos adicionales a la Policía Nacional: • Registro fotográfico antes de ejecución de mantenimiento. • Ubicación de equipos instalados. • Verificación de estado de los equipos. • Limpieza de equipos. • Mantenimiento de Equipos. • Cambio de equipos o repuestos de ser necesario. • Etiquetado de equipos. • Registro fotográfico después de ejecución de mantenimiento. • Realización de acta debidamente firmada por el responsable policial de cada sede. • Demás que sean necesarios para el correcto funcionamiento.		
10.3	Cada mantenimiento realizado a los servicios contratados descritos, el contratista deberá entregar al supervisor del contrato, acta por cada sede visitada, en donde se consigne las actividades de mantenimiento realizadas y descritas en el Ítem anterior, con recomendaciones técnicas para realizar futuros planes de mejora.		
10.4	En caso de requerirse un mantenimiento adicional a algún sitio descrito podrá ser solicitado por el supervisor del contrato cuando sea necesario, sin generar costos adicionales a la Policía Nacional.		

LOTE 2: CANALES DEDICADOS DE DATOS PARA LAS UNIDADES DE EMPADRONAMIENTO MODULAR.

ÍTEM	ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS				OFERTA/NO OFERTA
1	SERVICIO INTEGRAL DE SEGURIDAD PERIMETRAL, CONECTIVIDAD Y GESTIÓN DE RED, MEDIANTE LA IMPLEMENTACIÓN, CONFIGURACIÓN, OPERACIÓN Y SOPORTE DE UNA SOLUCIÓN BASADA EN TECNOLOGÍA SD-WAN, PARA LAS UNIDADES DE EMPADRONAMIENTO MODULAR.				
1.1	EL CONTRATISTA DEBERÁ SUMINISTRAR CANALES DE DATOS DEDICADOS, SOPORTADOS SOBRE INFRAESTRUCTURA DE FIBRA ÓPTICA E INTEGRADOS A LA SOLUCIÓN SD-WAN, DE ACUERDO CON LAS CAPACIDADES DEFINIDAS PARA CADA SEDE, ASÍ:				
	Nro.	**SEDE**	**DIRECCIÓN**	**CAPACIDAD**	
	1	**INDUMIL CAN – SEDE PRINCIPAL** MINISTERIO DE DEFENSA NACIONAL– BOGOTÁ D.C. **(NODO CENTRAL SD-WAN)**	CALLE 44 54-11 CAN	10 Mbps	
	2	**FÁBRICA DE ARMAS DE FUEGO JOSÉ MARÍA CÓRDOBA** INDUSTRIA MILITAR (INDUMIL) – SOACHA (CUNDINAMARCA)	CARRERA 17 30-211 SUR, CIUDAD LATINA	10 Mbps	

		3	**DÉCIMA TERCERA** SECCIONAL 16 USAQUÉN - BOGOTÁ D.C.	BRIGADA – CALLE 106 7A-25	10 Mbps		
		4	**SEPTIMA BRIGADA** SECCIONAL 27 VILLAVICENCIO – META	KILÓMETRO 1 VÍA PUERTO LÓPEZ	5 Mbps		
		5	**VIGÉSIMA TERCERA BRIGADA** SECCIONAL 77 PASTO	CALLE 22 14-47	5 Mbps		
		6	**CUARTA BRIGADA** SECCIONAL 45 MEDELLÍN	CARRERA 77C 51-182	5 Mbps		
		7	**QUINTA BRIGADA** SECCIONAL 55 BUCARAMANGA	CALLE 14 33A-127	5 Mbps		
		8	**SEGUNDA BRIGADA** **S**ECCIONAL 61 BARRANQUILLA	CALLE 58 59-136	5 Mbps		
		9	**OCTAVA BRIGADA** SECCIONAL 31 ARMENIA	AVENIDA BOLÍVAR 25N-00	5 Mbps		
		10	**TERCERA BRIGADA** SECCIONAL 73 CALI	CALLE 5 85-00	5 Mbps		
		11	**DECIMA SEGUNDA** SECCIONAL 83 FLORENCIA	CALLE 16 16-00	5 Mbps		
		LAS SEDES DE BOGOTÁ Y SOACHA CONTARÁ CON MAYOR CAPACIDAD DE ANCHO DE BANDA PARA SOPORTAR LA AGREGACIÓN DE TRÁFICO, LOS SERVICIOS CENTRALIZADOS DE SEGURIDAD PERIMETRAL Y LA GESTIÓN DE LA ARQUITECTURA SD-WAN.					
	1.2	La solución deberá estar basada en tecnología SD-WAN, permitiendo la gestión centralizada de la conectividad, la seguridad perimetral y la optimización del tráfico entre las sedes de la Entidad. La arquitectura deberá contemplar un hub central SD-WAN, el cual funcionará como nodo principal de agregación de tráfico, seguridad perimetral centralizada y gestión de la red, integrando los canales de datos de las diferentes sedes mediante conexiones seguras.					
	1.3	Los canales de datos deberán contar con velocidad simétrica, de acuerdo con las capacidades de ancho de banda definidas para cada sede, garantizando estabilidad, baja latencia y disponibilidad permanente del servicio.					
	1.4	Los servicios objeto del contrato deberán ser suministrados por un periodo mínimo de un (01) año, incluyendo garantía, soporte técnico especializado y operación continua durante toda la vigencia contractual.					
	1.5	**Redistribución dinámica de ancho de banda** La solución basada en tecnología SD-WAN deberá permitir la redistribución dinámica del ancho de banda contratado entre los diferentes canales de datos, de forma flexible y automática, sin afectar la disponibilidad general del servicio del contrato, permitiendo incrementar el ancho de banda en un canal específico mediante la disminución proporcional en otros, sin costo adicional y dentro del límite total contratado. El contratista deberá garantizar que dichos cambios se realicen previa solicitud formal de la Entidad y sean aplicados en un plazo no mayor a veinticuatro (24) horas, conforme a las políticas de gestión de red acordadas.					
	1.6	Los servicios deberán prestarse de manera continua, sin limitaciones funcionales, las veinticuatro (24) horas del día, durante toda la vigencia contractual.					
	1.7	El contratista deberá realizar la instalación, configuración, pruebas y puesta en operación de los servicios objeto del contrato en un plazo máximo de quince (15) días calendario, contados a partir de la aprobación de las pólizas					

		1.8	El contratista deberá proporcionar, instalar y configurar los equipos de borde y conectividad requeridos para la operación de la solución SD-WAN y los canales de datos dedicados, asegurando su correcto funcionamiento y disponibilidad permanente.		
		1.9	El contratista deberá suministrar los equipos de conectividad de borde (routers o dispositivos SD-WAN equivalentes) necesarios para garantizar el acceso seguro y permanente a la red principal de los canales de datos dedicados, así como realizar la instalación, configuración y ajustes requeridos para su correcto funcionamiento, una vez adjudicado el contrato.		
		1.10	La arquitectura de comunicaciones y conectividad implementada deberá operar de manera totalmente independiente de la red institucional de la Policía Nacional, garantizando su aislamiento lógico y físico, así como la no interferencia con los sistemas y servicios internos de la Entidad.		
		1.11	El contratista deberá suministrar los componentes de hardware y software necesarios que permitan la conectividad entre los nodos de la solución y los equipos ubicados en las sedes anteriormente informadas, garantizando su correcta instalación, integración y operación.		
		1.12	El contratista debe realizar la instalación y configuración de los servicios de la presente contratación, y soporte acordado con el supervisor del contrato. Debe cubrir a todo costo los componentes, cables de conexión y lo necesario para la funcionalidad que requiera el servicio.		
		1.13	El contratista deberá realizar la instalación, configuración y puesta en operación de los servicios objeto de la presente contratación, así como prestar el soporte técnico acordado con el supervisor del contrato. Deberá asumir a su costo el suministro de todos los componentes, equipos, accesorios, cables de conexión y demás elementos necesarios para garantizar la correcta funcionalidad y operación del servicio.		
		1.14	El contratista deberá garantizar la disponibilidad de los canales de datos durante toda la vigencia contractual, conforme a los niveles de servicio (ANS) establecidos en el presente documento.		
		1.15	El contratista deberá comprometer una disponibilidad mínima del servicio no inferior al noventa y nueve puntos siete por ciento (99.7 %) mensual, conforme a los Acuerdos de Nivel de Servicio (ANS) establecidos.		
		1.16	Si durante la ejecución del contrato se evidencia que el contratista no incluyó elementos, componentes o documentación necesarios para la correcta prestación de los servicios, este deberá suministrarlos, instalarlos, configurarlos y ponerlos en funcionamiento sin costo adicional para la Entidad. El hecho de que se detecten errores, inconsistencias u omisiones en los términos de referencia, pliegos o especificaciones técnicas no exime al contratista de la obligación de ejecutar de manera satisfactoria el objeto contractual dentro de los plazos establecidos, incluyendo las etapas de implementación, operación, soporte y garantía.		
		1.17	El contratista será responsable por los daños que se generen como consecuencia de una inadecuada instalación, manipulación o configuración de cualquier componente asociado al contrato, debiendo realizar a su costo las correcciones, adecuaciones, reparaciones e instalaciones necesarias para garantizar la correcta prestación de los servicios.		
		1.18	El contratista deberá disponer de personal técnico calificado, así como de los equipos, herramientas y recursos necesarios para dar cumplimiento integral al objeto contractual.		
		1.19	El contratista se obliga a cumplir los tiempos y actividades establecidos en el cronograma del proyecto, disponiendo de todos los medios, recursos técnicos y humanos necesarios para tal fin.		
		1.20	Todos los elementos requeridos para la puesta en operación del objeto contractual deberán ser nuevos. No se permitirá la reutilización de materiales o equipos usados.		
		1.21	Para las actividades de instalación de los componentes del proyecto no se podrán intervenir ni alterar elementos estructurales principales; el contratista deberá conservar las especificaciones y diseños de los componentes estructurales y arquitectónicos existentes.		
		1.22	Con el fin de garantizar un servicio adecuado, el contratista deberá suministrar el software necesario, debidamente licenciado, por el tiempo requerido durante la vigencia contractual.		

	1.23	El contratista deberá implementar los controles técnicos, administrativos y de seguridad necesarios para prevenir la fuga, pérdida o uso no autorizado de la información.		
	2	**SEGURIDAD**		
	2.1	El contratista deberá brindar soporte técnico durante toda la vigencia del contrato, conforme a los niveles de servicio establecidos.		
	2.2	El contratista se compromete a cumplir los lineamientos establecidos en la Resolución de Seguridad de la Información de la Policía Nacional y en el Manual del Sistema de Gestión de Seguridad de la Información (SGSI), o las normas que las modifiquen o sustituyan.		
	2.3	**Confidencialidad de la información** En virtud del presente contrato, el contratista se obliga a no suministrar, divulgar o utilizar información que obtenga o conozca con ocasión de su ejecución y que se encuentre clasificada como confidencial. Así mismo, el contratista deberá suscribir el acuerdo de confidencialidad exigido por la Entidad, comprometiéndose a la protección y no revelación de la información.		
	2.4	Cuando la Policía Nacional lo considere pertinente, el contratista permitirá y facilitará la realización de estudios de seguridad al personal que prestará los servicios, disponiendo los medios necesarios para tal fin.		
	2.5	Cuando la Policía Nacional lo considere pertinente, el contratista permitirá y facilitará la realización de estudios de seguridad al personal que prestará los servicios, disponiendo los medios necesarios para tal fin.		
	2.6	El contratista y su personal deberán cumplir las políticas de seguridad de la información, normas internas y demás disposiciones vigentes establecidas por la Policía Nacional relacionadas con la protección de la información y los activos institucionales.		
	2.7	El contratista y su personal que, con ocasión de la ejecución del contrato, conozcan métodos, procedimientos, información, infraestructura, doctrina, medios o productos propios de la Policía Nacional, estarán amparados por la reserva legal, conforme a lo dispuesto en la Ley 1581 de 2012, la Ley 1712 de 2014 y demás normas concordantes.		
	2.8	El contratista deberá diligenciar y suscribir el formato 1DT-FR-0016 “Declaración de Confidencialidad y Compromiso con la Seguridad de la Información – Contratistas o Terceros”, de conformidad con los lineamientos de la Entidad.		
	2.9	La información generada, procesada o administrada en desarrollo del presente contrato deberá manejarse bajo el principio de necesidad de conocer, garantizando su adecuada segmentación, acceso, uso y disposición final, conforme a los parámetros establecidos en la Ley 1581 de 2012, la Ley 1712 de 2014 y demás normas aplicables en materia de protección de datos e información institucional.		
	2.10	El contratista deberá dar cumplimiento a los lineamientos del Sistema de Gestión de Seguridad de la Información bajo el estándar ISO/IEC 27001 vigente o la norma que la modifique o sustituya.		
	2.11	El contratista será responsable de garantizar la legalidad y vigencia de las licencias de software utilizadas en la ejecución del contrato, manteniendo indemne a la Entidad frente a cualquier reclamación derivada de su uso.		
	3	**SOPORTE**		
	3.1	Los servicios objeto del contrato deberán contar con garantía y soporte técnico por un periodo mínimo de un (01) año, contado a partir del recibo a satisfacción de la Entidad, para todos los componentes implementados.		
	3.2	El contratista se compromete a actuar con diligencia ante cualquier novedad o falla que se presente en los servicios, adelantando las acciones necesarias para su restablecimiento durante toda la vigencia contractual.		
	3.3	El contratista deberá disponer de mínimo dos (02) canales de comunicación disponibles las veinticuatro (24) horas del día, los siete (7) días de la semana, a través de los cuales el supervisor del contrato podrá escalar requerimientos de soporte. Dichos canales de contacto deberán ser informados formalmente dentro de la documentación del proyecto.		

	3.4	El contratista deberá informar de manera oficial al supervisor del contrato el estado de gestión, solución y tiempos de atención de cada requerimiento de soporte escalado.		
	3.5	**(SLA de restablecimiento del servicio)** En caso de presentarse un evento de indisponibilidad del servicio, este deberá ser solucionado en un tiempo máximo de seis (06) horas, contadas a partir del reporte realizado a través de los canales de soporte establecidos.		
	3.6	**(Soporte presencial)** Cuando el soporte remoto no sea suficiente para la solución del incidente, el contratista deberá proporcionar atención presencial en las instalaciones correspondientes dentro de las seis (06) horas siguientes al reporte. Todos los costos asociados a la atención en sitio serán asumidos por el contratista		
	3.7	**(Responsabilidad por daños)** Los daños ocasionados durante la prestación del soporte técnico serán asumidos por el contratista, quien deberá subsanarlos y dejar los equipos o instalaciones en iguales o mejores condiciones, sin generar costos adicionales para la Entidad.		
	3.8	**(Reemplazo definitivo de equipos)** En caso de presentarse daños, defectos de fábrica o fallas recurrentes en los equipos instalados, el contratista deberá reemplazarlos por equipos nuevos de iguales o superiores características técnicas, sin costo adicional para la Entidad, durante toda la vigencia del contrato.		
	3.9	**(Equipo temporal de contingencia)** Cuando un equipo deba ser retirado para reparación o cambio por presentar inconvenientes técnicos, el contratista deberá instalar temporalmente un equipo de iguales o superiores características técnicas, garantizando la continuidad del servicio hasta su reposición definitiva.		
	4	**DOCUMENTACIÓN**		
	4.1	El contratista deberá suministrar certificación en la que se evidencie que los canales de datos son dedicados, de uso exclusivo, sin reuso, y con capacidades simétricas de subida y bajada.		
	4.2	El contratista deberá suministrar el esquema de conexión final de la infraestructura de red implementada, en el cual se detallen todos los componentes instalados.		
	4.3	El contratista deberá entregar la documentación técnica completa de los equipos, dispositivos y periféricos instalados, organizada mediante diagramas de conexión y fichas técnicas.		
	4.4	El contratista se compromete a entregar los manuales, guías de instalación, guías de usuario y toda la información técnica necesaria, en idioma español, para la correcta configuración, operación y uso de los sistemas implementados.		
	4.5	El contratista deberá entregar, al inicio del contrato, el cronograma de ejecución y el plan de trabajo para aprobación previa del supervisor del contrato.		
	4.6	El contratista deberá presentar los cronogramas de ejecución en diagrama de Gantt, en formato físico y digital. Dichos cronogramas deberán ser aprobados por el supervisor del contrato, y el pago estará condicionado a su entrega y al cumplimiento de los tiempos contractuales.		
	4.7	El contratista deberá suministrar la documentación que permita validar la prestación del servicio de canales de datos dedicados y sus características técnicas durante un periodo de un (01) año.		

	4.8	**PRESENTACIÓN DE LA OFERTA** El oferente deberá presentar junto con la oferta la siguiente documentación: **a)** Carta de presentación de la oferta, firmada por el representante legal de la empresa oferente, dirigida a la Dirección de Investigación Criminal e INTERPOL, en la cual se certifique: • Que los canales de datos ofertados cumplen con las capacidades solicitadas para cada una de las sedes durante un periodo mínimo de un (01) año. • Que los canales de datos son dedicados, de uso exclusivo, sin reuso y con capacidades simétricas de subida y bajada. • Relación de los canales de comunicación disponibles para el reporte de incidentes, conforme a lo establecido en el numeral 3.4. **b)** Certificado de partner vigente del fabricante de la solución SD-WAN y de los equipos de conectividad ofrecidos, que acredite autorización para comercialización, implementación y soporte técnico. **c)** Certificación de registro o habilitación ante el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), conforme a la normatividad vigente. **d)** Fichas técnicas de los equipos y soluciones ofrecidas, en las que se evidencien las características técnicas requeridas o superiores. La no presentación de cualquiera de los documentos técnicos exigidos en el presente numeral, incluyendo las fichas técnicas de los equipos y el certificado de partner del fabricante, será causal de rechazo de la oferta.		
	5	**GARANTIA**		
	5.1	El contratista deberá garantizar la disponibilidad continua de los servicios las veinticuatro (24) horas del día, los siete (07) días de la semana, durante toda la vigencia contractual. En caso de presentarse indisponibilidad atribuible al contratista, este deberá reponer el tiempo afectado, el cual será adicionado al plazo del contrato sin generar costos adicionales para la Entidad.		
	5.2	El contratista no podrá trasladar a terceros la responsabilidad derivada de la indisponibilidad del servicio, siendo el único responsable frente a la Entidad por el cumplimiento de los niveles de servicio.		
	5.3	El contratista deberá actuar con lealtad, diligencia y buena fe en todas las etapas contractuales, evitando dilaciones injustificadas o trabas en la ejecución del contrato.		
	5.4	La garantía de los servicios y componentes implementados tendrá una vigencia mínima de un (01) año, contado a partir del recibo a satisfacción por parte de la Entidad.		

CONDICIONES GENERALES CANALES DE DATOS DEDICADOS

NRO	CONDICIONES GENERALES PARA LA PRESTACIÓN DEL SERVICIO
1	**Visita Técnica** La Dirección de Investigación Criminal e INTERPOL, con el fin de facilitar a los oferentes el conocimiento de los aspectos técnicos y la finalidad de lo que se pretende adquirir por parte de la Entidad, programará una visita a los diferentes sitios anteriormente relacionados, en coordinación con el Jefe del Componente de Policía Científica y Criminalística y con el estructurador del estudio previo, con el propósito de verificar las condiciones técnicas establecidas en el presente proceso. La fecha y hora de la visita se establecerán en la Convocatoria Pública y en el pliego definitivo, los cuales serán publicados en la plataforma de Colombia Compra Eficiente, una vez se efectúe la apertura del proceso.

		Se aclara que dicha visita tendrá carácter informativo y no constituye requisito habilitante ni de obligatorio cumplimiento. Así mismo, se informarán oportunamente cambios en el cronograma por situaciones de orden público que impidan la realización de la actividad. **Nota:** La no asistencia a la visita técnica no exonera al proponente de su responsabilidad en la ejecución del contrato, ni podrá ser invocada como excusa para posteriores reclamaciones o incumplimientos contractuales. **Justificación:** La visita al sitio donde se desarrollará la adquisición de los servicios objeto del contrato permite al oferente conocer de primera mano las ubicaciones y condiciones donde se prestará el servicio, relacionadas en el presente proceso. La Dirección de Investigación Criminal e INTERPOL podrá reprogramar o cancelar la visita por motivos de seguridad.
	2	Los servicios deberán prestarse de manera continua, sin limitaciones funcionales, las veinticuatro (24) horas del día, durante toda la vigencia contractual.
	3	La arquitectura de comunicaciones y conectividad implementada deberá operar de manera totalmente independiente de la red institucional de la Policía Nacional, garantizando su aislamiento lógico y físico.
	4	Todos los componentes, equipos, accesorios y recursos necesarios para garantizar la conectividad y operación de los servicios serán suministrados por el contratista, sin generar costos adicionales para la Entidad.
	5	El contratista deberá garantizar la disponibilidad de los canales de datos durante toda la vigencia contractual, conforme a los niveles de servicio establecidos.
	6	El contratista deberá comprometer una disponibilidad mínima mensual del servicio no inferior al 99.7 %.
	7	El contratista será responsable por los daños que se generen como consecuencia de una inadecuada instalación, manipulación o configuración de cualquier componente del contrato.
	8	El contratista deberá disponer de personal técnico calificado, así como de los equipos, herramientas y recursos necesarios para el cumplimiento del objeto contractual.
	9	El contratista se obliga a cumplir los tiempos y actividades establecidos en el cronograma del proyecto.
	10	El contratista deberá suministrar los componentes de hardware y software necesarios para la implementación de la seguridad en red y la conectividad de la solución.
	11	Todos los elementos requeridos para la puesta en operación del objeto contractual deberán ser nuevos, sin reutilización de materiales o equipos usados.
	12	El contratista deberá suministrar el software requerido, debidamente licenciado, durante toda la vigencia contractual.
	13	Las actividades de instalación y mantenimiento deberán realizarse con acompañamiento autorizado por parte de la Policía Nacional.
	14	Los daños ocasionados durante la puesta en operación y prestación de los servicios serán asumidos por el contratista.
	15	El contratista deberá implementar controles de seguridad para prevenir la fuga o uso no autorizado de la información.
	16	El contratista deberá diligenciar y suscribir el formato institucional de confidencialidad.
	17	**SEGURIDAD**
	17.1	El contratista deberá brindar soporte técnico durante toda la vigencia del contrato.
	17.2	El contratista facilitará estudios de seguridad al personal cuando la Entidad lo requiera.
	17.3	El contratista cumplirá los compromisos de confidencialidad de la información.
	17.4	El contratista cumplirá el estándar ISO/IEC 27001 o la norma vigente aplicable.
	17.5	El contratista garantizará la legalidad y vigencia de las licencias de software.
	18	**SOPORTE**
	18.1	El contratista actuará con diligencia ante fallas del servicio.

	18.2	El contratista reportará oficialmente la gestión y solución de incidentes.
	18.3	El contratista garantizará soporte técnico especializado del proveedor o fabricante.
	18.4	El contratista reemplazará equipos por fallas recurrentes sin costo adicional.
	19	**DOCUMENTACIÓN**
	19.1	El contratista suministrará certificación de canales de datos dedicados y simétricos.
	19.2	El contratista entregará esquema final de conexión de la infraestructura de red.
	19.3	El contratista entregará documentación técnica completa de los equipos instalados.
	19.4	El contratista entregará manuales y guías técnicas en idioma español.
	19.5	El contratista entregará cronograma de ejecución y plan de trabajo.
	20	**GARANTÍA**
	21.1	El contratista no podrá trasladar a terceros la responsabilidad por la indisponibilidad del servicio.
CONDICIONES DE CONTRATACIÓN	***OBLIGACIONES DEL CONTRATISTA***	**1.** Cumplir con el objeto contractual. **2.** Garantizar la disponibilidad del servicio los siete (07) días de la semana las veinticuatro (24) horas del día durante la vigencia del servicio. En caso de presentarse indisponibilidad del servicio, el contratista repondrá el tiempo, siendo adicionado a la fecha de finalización del contrato sin que se genere un costo adicional para la Policía Nacional. **3.** El contratista no trasladará a terceros la responsabilidad que se pueda generar ante la indisponibilidad del servicio. **4.** Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas. **5.** Responder en los plazos que la POLICÍA NACIONAL establezca en cada caso, los requerimientos de aclaración o de información que le formule. **6.** Cumplir cabalmente con sus obligaciones, frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por cuanto el cumplimiento de esta obligación es requisito indispensable para la realización de cualquier pago. **7.** Constituir en debida forma y aportar al Grupo de contratos del Área Logística y Financiera de la Dirección de Investigación Criminal e INTERPOL o quien haga sus veces, dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, la Garantía Única. **8.** Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y utilización indebida que por sí o por un tercero se cause a la administración o a terceros. **9.** No acceder a peticiones o amenazas, de quienes actuando por fuera de la ley pretendan obligarlo a hacer u omitir algún acto o hecho, el CONTRATISTA deberá Informar de tal evento a la Dirección de Investigación Criminal e INTERPOL de la Policía

		Nacional y a las autoridades competentes para que se adopte las medidas necesarias. **10.** Mantener activa la cuenta corriente o de ahorros reportada para los pagos con el fin de evitar traumatismos en el proceso de ejecución del contrato. **11.** Restituir a LA POLICÍA NACIONAL los elementos que haya colocado a su disposición para el desarrollo del objeto contractual, cuando se lo requiera o al finalizar el contrato, en caso de que se hayan suministrado. **12.** Para la facturación de los bienes o servicios contratados, se debe tener en cuenta los lineamientos y parámetros contemplados en la circular externa 016 del 09 de marzo de 2021 establecidos por el Ministerio de Hacienda y Crédito Público, por medio del cual se implementa el modelo de recepción de facturas de venta, notas débito y/o notas crédito, la cual es de obligatorio cumplimiento, de acuerdo con la Directiva Presidencial 09 del 17 de septiembre de 2020 "*Lineamientos para el Pago de Proveedores del Estado*" y la Resolución No. 000042 del 05 de mayo de 2020, "*Por la cual se desarrollan los sistemas de facturación, los proveedores tecnológicos*" y el registro de la factura electrónica de venta. **13.** Las demás obligaciones del CONTRATISTA contenidas en el artículo 5º de la Ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual. **14.** Al momento que los contratistas ingresen a las instalaciones deberán tener un acompañante para el desplazamiento. **15.** Es responsabilidad del contratista suministrar los elementos necesarios para portar una identificación visible dentro de las instalaciones de la Dirección de Investigación Criminal e INTERPOL, cumpliendo con los controles de acceso físico a instalaciones policiales (carné). **16.** Iniciada la etapa de ejecución contractual, el promotor de seguridad de la información del Grupo Recepción y Análisis de Comunicaciones Interceptadas, deberá dar instrucciones al contratista del Sistema de Gestión y Seguridad de la Información, de acuerdo a lo establecido en el control A.1.6.3 "conciencia de seguridad de la información, educación y formación". Se deberá enviar el soporte de la actividad al Grupo de Protección de Datos y Seguridad de la Información DIJIN. **17.** Se debe incorporar y dar cumplimiento al control A.1.5.19 "seguridad de la información en las relaciones con proveedores" de la norma ISO 27001:2022 Sistema de Gestión de Seguridad de la Información. **18.** Los contratistas deberán diligenciar el formato 1DT-FR-0016 "Declaración de confidencialidad y compromiso con la seguridad

		de la información contratistas o terceros", y enviar por correo electrónico copia del formato 1DT-FR-0016 al Grupo de Protección de Datos y Seguridad de la Información debidamente diligenciado. **19.** La información confidencial intercambiada entre las partes será tratada con la máxima confidencialidad y protegida contra el acceso no autorizado, la divulgación, la modificación o la destrucción, en cumplimiento al control A.1.6.6 "acuerdos de confidencialidad o no divulgación". **20.** Se deberá dar cumplimiento al control A.1.6.5 "Retiro o ajustes de los derechos de acceso" se eliminarán los derechos de accesos de todos los empleados y usuarios externos a la información y a las instalaciones de procedimiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. **21.** Se deberá elaborar y mantener relacionado en el inventario de activos de la Dirección de Investigación Criminal e INTERPOL, los elementos adquiridos, establecido en el control A.1.5.9. "Inventario de información y otros activos asociados". **22.** Es fundamental que el contratista sea consciente de las consecuencias de no cumplir con los requisitos de la seguridad de la información en la Dirección de Investigación Criminal e INTERPOL y sepa cuáles son las acciones correspondientes a tomar en caso, de no respetarlas, por lo que es necesario que el contratista sea diligente en su cumplimiento. **23.** En caso de vulneración a la seguridad de la información se llevará a cabo una auditoría de seguridad de la información, y se establecerán controles de monitoreo para detectar y responder rápidamente a cualquier violación de seguridad. **24.** Reportar inmediatamente cualquier incidente de seguridad, incluyendo robo, pérdida, o acceso no autorizado a los datos, a la persona responsable de la seguridad de la información en la Dirección de Investigación Criminal e INTERPOL, en cumplimiento al control A.1.5.26 "respuestas a incidentes de seguridad de la información". **CONCEPTO SEGURIDAD DE LA INFORMACIÓN.** • Al momento que los contratistas ingresen a las instalaciones deberán tener un acompañante para el desplazamiento. • Es responsabilidad del contratista suministrar los elementos necesarios para portar una identificación visible dentro de las instalaciones de la Dirección de Investigación Criminal e INTERPOL, cumpliendo con los controles de acceso físico a instalaciones policiales (carné). • Iniciada la etapa de ejecución contractual, el promotor de seguridad de la información del Grupo de Recepción y Análisis

		de Comunicaciones Interceptadas, deberá dar instrucciones al contratista del Sistema de Gestión y Seguridad de la Información, de acuerdo a lo establecido en artículo 84 *"Conciencia de seguridad de la información, educación y formación"*. Se deberá enviar el soporte de la actividad al Grupo de Protección de Datos y Seguridad de la Información DIJIN. • Se deberá atender las directrices emitidas para el uso correcto de la información de acuerdo a los niveles de clasificación adoptados por la institución, en cumplimiento al artículo *15 "Uso aceptable de la información y otros activos asociados"*. • Se deberá dar cumplimiento al artículo 25 *"Acuerdos con los proveedores"*, el supervisor de cada contrato o convenio, será el responsable de divulgar la política y lineamientos de seguridad de la información; los contratistas deberán diligenciar el formato 1DT-FR-0016 *"Declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros"*, y enviar por correo electrónico copia del formato 1DT-FR-0016 al Grupo de Protección de Datos y Seguridad de la Información debidamente diligenciado. • Se deberá dar cumplimiento al artículo 27 *"Continuidad del negocio"*, disponiendo de planes necesarios para la continuidad de la operación de los servicios tecnológicos, lo cuales serán operados por los líderes de los procesos. • La información confidencial intercambiada entre las partes será tratada con la máxima confidencialidad y protegida contra el acceso no autorizado, la divulgación, la modificación o la destrucción, en cumplimiento al artículo 30 *"Confidencialidad o de no divulgación".* • Se deberá garantizar lo estipulado en el artículo 36 *"Operaciones de protección de los activos de información"*, velando por la eficiencia de los controles asociados a los recursos tecnológicos, protegiendo la disponibilidad, integridad y confidencialidad de la información, para que los cambios efectuados sobre los recursos tecnológicos de los sistemas de información, en ambientes de prueba y producción sean controlados y autorizados. • Se deberá elaborar y mantener relacionado en el inventario de activos de la Dirección de Investigación Criminal e INTERPOL, los elementos adquiridos, establecido en el artículo 59 *"Inventario de información y otros activos asociados"*. • Se debe incorporar y dar cumplimiento al artículo 60 *"Devolución de activos"*, los funcionarios activos, personal no uniformado, contratistas o quienes hayan recibido activos de información institucionales para el cumplimiento de sus funciones, son responsables de la devolución de los mismos en el momento de registrar novedad administrativa temporal o definitiva de la institución. • Se deberá dar cumplimiento al artículo 65 *"Derechos de acceso"* se eliminarán los derechos de accesos de todos los empleados y

		usuarios externos a la información y a las instalaciones de procedimiento de información, se deben retirar al terminar su empleo mediante paz y salvo electrónico. • Se debe incorporar y dar cumplimiento al artículo 66 *"Seguridad de la información en la relación con proveedores"*, quienes la firma de contratos, acuerdo o convenios con el personal externo deben garantizar el cumplimiento del Manual de Seguridad de la Información. • Reportar inmediatamente cualquier incidente de seguridad, incluyendo robo, pérdida, o acceso no autorizado a los datos, a la persona responsable de la seguridad de la información en la Dirección de Investigación Criminal e INTERPOL, en cumplimiento al artículo 69 *"Respuesta a incidentes de seguridad de la información".* • Se debe incorporar y dar cumplimiento al artículo 94 *"Emplazamiento de los equipos"*, establece que los equipos de cómputo deben ubicarse y protegerse de manera que se minimicen los riesgos por amenazas ambientales y accesos no autorizados, lo cual implica que los centros de procesamiento cumplan la norma ANSI/TIA 942, que los servidores se agrupen en áreas con estrictos controles de acceso físico, que la disposición de los equipos evite la visualización indebida de información, que el ingreso a estas áreas sea restringido y debidamente trazado, y que los centros de datos cuenten con controles ambientales que reduzcan la probabilidad de pérdida de información. • Se deberá garantizar lo estipulado en el artículo 96 *"Servicios públicos de apoyo"*, las unidades que soportan sistemas de información, aplicaciones y componentes críticos de la plataforma tecnológica institucional en producción, deben asegurar que se cuente con protección ante interrupciones causadas por fallos en los servicios públicos de apoyo. • Es fundamental dar cumplimiento al artículo 97 *"Seguridad en el cableado"*, en el cual se establece que el cableado eléctrico y de comunicaciones debe cumplir con el RETIE y los estándares ISO/IEC 11801 y ANSI/EIA/TIA 568A o 568B, garantizando protección contra daños externos, conexión de sus partes metálicas al sistema de tierras, y almacenamiento de equipos en ambientes entre 16 y 22 °C. Además, los centros de cableado deben contar con racks seguros administrados por personal técnico, y las instalaciones deben ajustarse a la arquitectura del edificio, usando canaletas en interiores o tubería metálica para instalaciones a la intemperie. • Se deberá garantizar la disponibilidad, integridad y confidencial de la información, dando cumplimiento al artículo 98 *"Mantenimiento de equipos".* • Es fundamental dar cumplimiento al artículo 111 *"Redundancia de las instalaciones de procesamiento de información,"* el cual

establece que las unidades de policía responsables de sistemas de información y componentes tecnológicos críticos deben garantizar la implementación de mecanismos de redundancia que aseguren la disponibilidad continua de los servicios institucionales.

- Se deberá dar cumplimiento al artículo 126 *"Gestión de cambio",* con el fin de que los cambios y procedimientos dentro del ciclo de vida del desarrollo de los sistemas de información, sean controlados formalmente mediante el procedimiento de gestión de cambios.

- Es fundamental que el contratista sea consciente de las consecuencias de no cumplir con los requisitos de la seguridad de la información en la Dirección de Investigación Criminal e INTERPOL y sepa cuáles son las acciones correspondientes a tomar en caso, de no respetarlas, por lo que es necesario que el contratista sea diligente en su cumplimiento.

- En caso de vulneración a la seguridad de la información se llevará a cabo una auditoría de seguridad de la información, y se establecerán controles de monitoreo para detectar y responder rápidamente a cualquier violación de seguridad.

De igual forma, se recomienda que en la gestión del proyecto se evalúen los riesgos de seguridad de la información asociados al mantenimiento de equipos, conforme a ISO/IEC 27001:2022, así:

Riesgo	Vulnerabilidad	Controles ISO/IEC 27001:2022
Divulgación no autorizada de estudios previos, presupuesto oficial y documentos precontractuales.	Ausencia de clasificación de información y controles de acceso débiles.	A.5.12 Clasificación de la información, A.5.13 Etiquetado de información, A.5.15 Control de acceso.
Acceso no autorizado a expedientes electrónicos del proceso contractual.	Gestión inadecuada de usuarios y privilegios.	A.5.15 Control de acceso, A.8.2 Derechos de acceso privilegiado, A.8.3 Restricción de acceso a la información.
Modificación no autorizada de especificaciones técnicas del servicio MPLS e Internet.	Falta de control de versiones y trazabilidad documental.	A.8.15 Registro de eventos, A.8.16 Monitoreo de actividades, A.8.32 Gestión de cambios.
Filtración de información sobre la infraestructura tecnológica de la DIJIN.	Compartición excesiva de información técnica con terceros.	A.5.14 Transferencia de información, A.5.12 Clasificación de la información, A.8.24 Uso de criptografía.
Manipulación de estudios de mercado o análisis sectoriales.	Validación insuficiente de la información recibida.	A.5.19 Seguridad en relaciones con proveedores, A.5.21 Gestión de riesgos en la cadena de suministro TIC.
Ataques de ingeniería social contra funcionarios que participan en el proceso.	Bajo nivel de concienciación en seguridad.	A.6.3 Concienciación, educación y formación en seguridad de la información, A.6.8 Reporte de eventos de seguridad.
Suplantación de identidad de proveedores o funcionarios.	Mecanismos de autenticación insuficientes.	A.8.5 Autenticación segura, A.5.16 Gestión de identidad.

Pérdida de documentos electrónicos de la contratación.	Ausencia de respaldos y procedimientos de recuperación.	A.8.13 Copias de seguridad de la información, A.5.30 Preparación TIC para la continuidad del negocio.
Interrupción de plataformas utilizadas para la gestión contractual (SECOP, correo institucional, repositorios).	Dependencia tecnológica sin planes de contingencia.	A.5.30 Preparación TIC para la continuidad del negocio, A.5.29 Seguridad durante interrupciones.
Divulgación de credenciales institucionales utilizadas en el proceso.	Contraseñas débiles o compartidas.	A.5.17 Información de autenticación, A.8.5 Autenticación segura.
Instalación de software malicioso mediante archivos compartidos por terceros.	Ausencia de controles antimalware y verificación de archivos.	A.8.7 Protección contra malware, A.8.23 Filtrado web.
Alteración o eliminación accidental de información contractual.	Errores humanos y falta de controles de cambios.	A.8.32 Gestión de cambios, A.8.10 Eliminación de información.
Uso de canales no autorizados para el intercambio de información con proveedores.	Falta de lineamientos para transferencia segura.	A.5.14 Transferencia de información, A.8.24 Criptografía.
Conflicto de interés o intervención indebida en la elaboración de requisitos técnicos.	Segregación insuficiente de funciones.	A.5.2 Roles y responsabilidades de seguridad, A.5.3 Segregación de funciones.
Ataque cibernético dirigido a repositorios documentales institucionales.	Monitoreo y protección insuficiente de activos de información.	A.8.16 Monitoreo de actividades, A.8.20 Seguridad de redes, A.8.7 Protección contra malware.
Contratación de un proveedor con debilidades en seguridad de la información.	Debida diligencia insuficiente durante la evaluación de oferentes.	A.5.19 Seguridad en relaciones con proveedores, A.5.20 Gestión de la seguridad en acuerdos con proveedores, A.5.22 Monitoreo de servicios de proveedores.
Exposición de información reservada en mesas de trabajo o reuniones de socialización.	Falta de acuerdos de confidencialidad y control de asistentes.	A.6.6 Acuerdos de confidencialidad, A.5.14 Transferencia de información.
Fuga de información por dispositivos portátiles utilizados por el equipo estructurador.	Equipos sin cifrado o controles de protección.	A.8.1 Dispositivos de usuario final, A.8.24 Uso de criptografía.

REQUISITOS AMBIENTALES A INCLUIRSE EN EL CONTRATO.

Requisitos en materia ambiental:

En atención a lo contemplado en la Nota 4 de la Resolución nro. 03049 del 2014 *"Por la cual se adopta el Manual de Contratación de la Policía Nacional"*, complementada por el Numeral 5 del apéndice de la Resolución Nro. 00090 del 2018 *"Por la cual se actualiza, modifica y complementa el manual de contratación de la Policía Nacional"* adoptado mediante Resolución 03049 de 2014, o norma que adicione, sustituya o modifique; se deberán tener en cuenta las siguientes consideraciones, así:

		Criterios para compras públicas sostenibles Con el objeto de cumplir con la normativa ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a su actividad productiva, los contratistas deberán presentar los permisos o licencias que dieron lugar para el funcionamiento de su compañía y el desarrollo de su actividad productiva; cualquier infracción ambiental por omisión de permisos, concesiones o licencias ambientales que hubiese sido necesario tramitar antes del inicio del contrato, en el transcurso y después de la actividad del proceso, serán asumidas como responsabilidad del contratista. **3. Criterios ambientales en los contratos de prestación de servicios.** Se deberá impartir, instrucciones, socializaciones y/o capacitaciones al personal bajo su cargo en temas ambientales relacionados con sus aspectos e impactos ambientales estableciendo y presentando cronograma en temas tales como: • Gestión integral de residuos sólidos y líquidos, con medidas que permitan disminuir la cantidad de residuos generados. • Uso de elementos de protección personal. • Ahorro y uso eficiente de recursos (agua y energía). • Normativa ambiental. • Saneamiento básico. • Gestión del riesgo asociado a su actividad productiva. **5. Criterios en materia de pos - consumo** Serán aplicables según corresponda, a los contratos de adquisición de componentes que una vez cumplen con su ciclo de vida útil, generen los siguientes residuos, *"RESIDUOS DE APARATOS ELÉCTRICOS Y ELECTRÓNICOS, RAES"*. **5.4 RAEES** De aplicar, el futuro contratista deberá cumplir con las obligaciones fijadas para productores por la **Resolución 1512 del 2010**, *"Por la cual se establecen los Sistemas de Recolección Selectiva y Gestión Ambiental de Residuos de Computadores y/o Periféricos y se adoptan otras disposiciones"*, expedida por el Ministerio de Ambiente, o aquella norma que la modifique, adicione o sustituya, para lo cual deberá presentar la aprobación ante la autoridad ambiental competente del Sistemas de Recolección Selectiva y Gestión Ambiental de Residuos de Computadores y/o Periféricos que posea o este participando y enviar a la respectiva unidad policial, los lineamientos y procedimientos para su participación como consumidores. **Obligaciones del contratista** • Realizar la separación en la fuente de los residuos generados durante la instalación y acondicionamiento. • Garantizar la recolección, transporte y disposición final de los residuos por gestores autorizados cuando aplique. • Mantener evidencia documental de la entrega de residuos reciclables, especiales o peligrosos a gestores autorizados. • Evitar el abandono o disposición inadecuada de residuos. • Participar de los programas y campañas ambientales implementados en la Dirección.

		Manejo de residuos de adecuación física (Obra). Si durante la instalación se generan escombros, materiales sobrantes, residuos de perforaciones, cableado o adecuaciones locativas menores, el contratista deberá efectuar su manejo y disposición de conformidad con las disposiciones sobre Residuos de Construcción y Demolición conforme a la normatividad vigente. **Uso eficiente de recursos, el contratista deberá adoptar medidas para** • Minimizar el consumo de energía eléctrica. • Optimizar el uso de agua durante las actividades de instalación. • Reducir la generación de residuos. • Promover la reutilización y reciclaje de materiales de empaque y embalaje. **Obligaciones Ambientales aplicables** • Declarar cumplimiento de la normatividad ambiental vigente. • No tener sanciones ambientales vigentes • Utilizar equipos con funciones de eficiencia energética. • Gestionar adecuadamente los RAEE mediante gestores autorizados. • Realizar mantenimiento preventivo que optimice el consumo energético. • Priorizar la entrega de informes y soportes en formato digital para reducir consumo de papel, *"**Directiva Presidencial 04 de 2012** Política Cero Papel"*. **Riesgos ambientales a verificar en el seguimiento contractual** • Generación de residuos electrónicos por cambio de routers, switches, módems o equipos de transmisión. • Disposición inadecuada de equipos tecnológicos fuera de uso. • Incremento del consumo energético por utilización de equipos sin eficiencia energética. • Falta de soportes de gestión posconsumo de equipos retirados. **Verificación y Soporte del Cumplimiento Ambiental:** El supervisor deberá verificar, efectuar seguimiento y dejar evidencia del cumplimiento de los requerimientos y obligaciones ambientales establecidos en el estudio de conveniencia y oportunidad para los contratos o convenios, los cuales podrán ser objeto de revisión en ejercicios de supervisión y control. Dicho seguimiento deberá quedar debidamente registrado en el formato 2BSFR-0019 *"Informe de Supervisión Seguimiento Contractual"*, el cual será presentado al ordenador del gasto, garantizando así el cumplimiento de la normatividad ambiental vigente. **Seguimiento y Control del Cumplimiento:** Los supervisores designados en los contratos o convenios deben realizar un seguimiento continuo y controlar que las obligaciones ambientales sean respetadas durante toda la ejecución del contrato.

		Requisitos Informativos en materia ambiental: El contratista deberá informar si cuenta con reconocimientos ambientales vigentes, especificando, en caso afirmativo, la entidad que los otorga, la fecha, el nombre del reconocimiento y su justificación. Asimismo, deberá indicar si el contrato a prestar *"ADQUISICIÓN DE SERVICIOS DE CANALES DEDICADOS MPLS Y DE INTERNET PARA LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL"*, cuenta con certificaciones ambientales o si se encuentra alineado con indicadores de desempeño que evidencien condiciones de favorabilidad y confiabilidad ambiental, así como acreditar si sus proveedores cuentan con certificación ISO 14001 o han sido reconocidos por autoridades ambientales por su compromiso con la protección y conservación del medio ambiente. **Proceso de supervisión:** El proceso de supervisión es clave para garantizar que el contrato no solo se cumpla en términos operativos, sino también que se respeten las normativas y compromisos ambientales establecidos.
	FORMA DE PAGO	La Dirección de Investigación Criminal e INTERPOL se obliga a cancelar el valor del contrato que se derive de la presente contratación en pesos colombianos en la Ciudad de Bogotá en un (01) pago por lote completo, correspondiente a la entrega a satisfacción del servicio adquirido. En todo caso, el pago se realizará previo cumplimiento del objeto contractual, una vez emitida la respectiva factura y demás documentos requeridos por esta Dirección; (cuando los elementos sean de origen extranjero se deberá aportar la declaración de importación) el pago se realizará dentro de los sesenta (60) días siguientes a la radicación de la factura, según programación de PAC por parte del Ministerio de Hacienda y Crédito Público y asignación de turno correspondiente, de conformidad con lo establecido en el Artículo 19 de la Ley 1150 de 2007 Derecho a Turno se le asignará el respectivo turno de pago.
	RIESGO DE LA CONTRATACIÓN	En el texto de la Póliza Única de Garantía se dejará expresa constancia que se ampara el cumplimiento del contrato, el valor de las multas y la cláusula penal pecuniaria convenida.
	MECANISMO DE COBERTURA DE LOS RIESGOS	los mecanismos de cobertura de riesgo establecidos en el Decreto 4828 de fecha diciembre 24 de 2008, que cubra los siguientes riesgos: **- DE CUMPLIMIENTO DEL CONTRATO:** Por el VEINTE por ciento (20%) del valor total del contrato, con una vigencia igual a la vigencia del contrato y SESENTA (60) días calendario más, con inicio en la fecha de suscripción del contrato y de las prórrogas si las hubiere. **- CALIDAD DEL SERVICIO:** por el CINCUENTA por ciento (50%) del valor del contrato, con una vigencia igual a la vigencia del contrato y un año más, con inicio en la fecha de suscripción del contrato y de las prórrogas si las hubiere. **- NO PAGO DE SALARIOS, PRESTACIONES E INDEMNIZACIONES LABORALES:** por el CINCO por ciento (5%) del valor del contrato, con una vigencia igual a la vigencia del contrato y tres años más, con inicio en la fecha de suscripción del contrato y de las prórrogas si las hubiere.

VALOR OFRECIDO

En este campo debe ir la indicación específica de que quien cotiza deberá tener en cuenta todos los gastos en los que incurra por la suscripción, legalización y ejecución del contrato, como impuestos, publicaciones, constitución garantía única, transporte, operarios, etc.

LOTE 1: ADQUISICIÓN DE SERVICIO DE CANALES DEDICADO MPLS Y DE INTERNET PARA LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL.

ÍTEM	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO INCLUIDO IVA.	VALOR TOTAL INCLUIDO IVA.
1	CANAL DEDICADO INTERNET DE 100 Mbps CARRERA 62 # 19-04 INT 1 ZONA INDUSTRIAL-PUENTE ARANDA BOGOTÁ-CUNDINAMARCA.	01	$ -	$ -
2	CANAL DEDICADO MPLS DE 500 Mbps CARRERA 62 # 19-04 INT 1 ZONA INDUSTRIAL-PUENTE ARANDA BOGOTÁ-CUNDINAMARCA. CANAL PRINCIPAL.	01	$ -	$ -
3	CANAL DEDICADO MPLS DE 250 Mbps AV. EL DORADO # 75 - 25 MODELIA BOGOTÁ-CUNDINAMARCA. DISASTER RECOVERY (DR).	01	$ -	$ -
4	CANAL DEDICADO MPLS DE 100 Mbps –SACOM2. CALLE 21 SUR # 6 – 235 - ZONA INDUSTRIAL - REGIONAL DE POLICIA Nº2.	01	$ -	$ -
5	CANAL DEDICADO MPLS DE 100 Mbps – SACOM3. AV. DE LAS AMERICAS # 46 - 35 - COMANDO DE POLICIA METROPOLITANA DE PEREIRA.	01	$ -	$ -
6	CANAL DEDICADO MPLS DE 100 Mbps – SACOM4. AV. PANAMERICANA # 1N - 75 BARRIO VILLA PAULA - COMPLEJO POLICÍA IJ DIEGO GUERRERO POPAYÁN - CAUCA.	01	$ -	$ -
7	CANAL DEDICADO MPLS DE 100 Mbps – SACOM5. TRANSVERSAL 203 # 27ª - 01 VÍA RUITOQUE BAJO KILOMETRO 1 - COMPLEJO POLICÍA NACIONAL FUERTE SUR FLORIDABLANCA-SANTANDER.	01	$ -	$ -
8	CANAL DEDICADO MPLS DE 100 Mbps – SACOM6. CALLE 72 # 64 - 70 BARRIO CARIBE - SIJIN MEVAL MEDELLÍN – ANTIOQUIA.	01	$ -	$ -
9	CANAL DEDICADO MPLS DE 100 Mbps – SACOM7. CALLE 44 # 35C - 02 - EL TRIUNFO-COMANDO POLICIA META.	01	$ -	$ -
10	CANAL DEDICADO MPLS DE 100 Mbps – SACOM8. CALLE 74 # 38 - 13 - LAS DELICIAS - COMPLEJO REGIONAL DE CRIMINALISTICA Nº8.	01	$ -	$ -
11	CANAL DEDICADO MPLS DE 100 Mbps – SACOM MECAL. CALLE 21 # 1N - 65 - BARRIO PILOTO - COMANDO POLICIA METROPOLITANA DE CALI.	01	$ -	$ -

LOTE 2: CANALES DEDICADOS DE DATOS PARA LAS UNIDADES DE EMPADRONAMIENTO MODULAR.

ÍTEM	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO INCLUIDO IVA.	VALOR TOTAL INCLUIDO IVA.
1	INDUMIL CAN – SEDE PRINCIPAL MINISTERIO DE DEFENSA NACIONAL– BOGOTÁ D.C. (NODO CENTRAL SD-WAN)	01	$ -	$ -
2	FÁBRICA DE ARMAS DE FUEGO JOSÉ MARÍA CÓRDOBA INDUSTRIA MILITAR (INDUMIL) – SOACHA (CUNDINAMARCA)	01	$ -	$ -
3	DÉCIMA TERCERA SECCIONAL 16 USAQUÉN - BOGOTÁ D.C.	01	$ -	$ -
4	SEPTIMA BRIGADA	01	$ -	$ -

		SECCIONAL 27 VILLAVICENCIO – META			
	5	VIGÉSIMA TERCERA BRIGADA SECCIONAL 77 PASTO	01	$ -	$ -
	6	CUARTA BRIGADA SECCIONAL 45 MEDELLÍN	01	$ -	$ -
	7	QUINTA BRIGADA SECCIONAL 55 BUCARAMANGA	01	$ -	$ -
	8	SEGUNDA BRIGADA SECCIONAL 61 BARRANQUILLA	01	$ -	$ -
	9	OCTAVA BRIGADA SECCIONAL 31 ARMENIA	01	$ -	$ -
	10	TERCERA BRIGADA SECCIONAL 73 CALI	01	$ -	$ -
	11	DECIMA SEGUNDA SECCIONAL 83 FLORENCIA	01	$ -	$ -
PLAZO PARA PRESENTAR COTIZACIONES	El plazo para remitir la cotización es de tres días hábiles contados desde que reciba el correo donde se notifica y debe ser enviado por cualquiera de los siguientes medios, así: dijin.graco-sop@policia.gov.co Conmutador: 5159700 Ext. 30474 Celular 3228443232				