Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
1	**SOFTWARE Y HARDWARE**		
1.1	**Marca:**		
1.2	Herramienta de análisis comportamental en la WAN (red de área amplia), la cual incluye equipo y software, herramienta que debe ser basada en modelos matemáticos y probabilísticos (no firmas), que le permita contar con un aprendizaje automático (de la Red de la Policía Nacional) que no necesite la supervisión de la entidad para él envío de alertas, estas deben ser cambiantes de acuerdo a la probabilidad de que el comportamiento del usuario pueda estar fuera de los rangos normales. Adicional a esto, la solución a renovar debe tener la capacidad de extender la visibilidad del tráfico de red de los dispositivos que no se encuentren bajo la red LAN, y que sean de prioridad para la organización como mínimo de cien (100) endpoints. Auto aprendizaje basado en algoritmos de machine learning no supervisado, debe iterar constantemente verificando el uso normal de la red. Para políticas de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de la Policía Nacional, la herramienta debe permitir a través de su algoritmo de maching learning (Clasificación de datos con base en reglas específicas de negocio).		
1.3	La herramienta deberá utilizar modelos matemáticos de estimación recursiva bayesiana o similares con el fin de validar los comportamientos anormales en la red.		
1.4	La herramienta deberá basar sus detecciones en el comportamiento de la red de la Policía Nacional, para de esta forma detectar amenazas conforme surgen (tiempo real).		
1.5	La herramienta deberá revisar y analizar el comportamiento de usuarios, dispositivos y redes de forma automática, no deben ser pre configurados los rangos a escanear, conforme van siendo analizados por la herramienta, estos deben hacer parte del inventario.		
1.6	La herramienta deberá poder reconocer información en ambientes virtualizados con hyperv, equipos de cómputo con sistemas operativos Windows XP (sp3), Windows 7 (sp1), Windows 7 (sp1) x64, Windows 8 Windows 10, Windows 11, Linux y MacOS.		
1.7	La actualización del software de maching learning, no deberá depender de un procedimiento del administrador este se debe actualizar constantemente.		
1.8	La herramienta deberá soportar los siguientes modos de implementación: Terminal Access Point (TAP) Port mirror (SPAN) En el caso que se instale en modo TAP, la red de la Policía Nacional debe mantener en idénticas condiciones de velocidad en la navegación, el equipo no debe introducir delays (retardos) de tiempo en la red.		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	El sistema se configura en modo bypass cuando lo desee el administrador del sistema.		
1.9	La herramienta deberá ser instalada y gestionada en sitio, no se aceptan soluciones que necesiten de la nube para hacer los análisis de la información, cualquier configuración remota debe ser consultada y autorizada con la Policía Nacional.		
1.10	La herramienta deberá contar con la capacidad de integración con el correlacionador de eventos (SIEM), que la institución tenga implementado.		
1.11	La Herramienta deberá enviar notificaciones en múltiples métodos y formatos. Si se utiliza Syslog, SNMP, o email, las notificaciones deben contener toda la data necesaria.		
1.12	La herramienta deberá contar con un dashboard que permita visualizar en tiempo real todos los detalles técnicos de la posible amenaza como son: dirección IP, tipo de amenaza, gravedad, nombre de máquina, usuario, tipo de amenaza con su descripción.		
1.13	La herramienta deberá permitir acceder a la trazabilidad de una amenaza y visualizar el histórico de una amenaza puntual, que tenga categoría de incidente.		
1.14	Las amenazas reportadas deben ser agrupadas de acuerdo a su tipo con el fin de optimizar el análisis del investigador.		
1.15	La herramienta deberá tener la capacidad de visualizar la topología de red que va descubriendo, esta debe ser dinámica si se da un click sobre uno de estos elementos, arrojando información detalla del tipo de dispositivo.		
1.16	La herramienta deberá entregar un resumen del comportamiento general de los dispositivos e IPs externas y uso de los protocolos más importantes como HTTP, POP3, SMTP, KERBEROS, FTP y DNS.		
1.17	La herramienta deberá ser tipo appliance.		
1.18	La administración de la herramienta deberá realizarse tipo web, en el caso que la solución de administración sea cliente servidor el licenciamiento debe ser ilimitado. Igualmente, se debe poder tener visualización de las alertas por medio de una aplicación móvil nativa de la herramienta.		
1.19	La Herramienta deberá permitir la definición de roles de administración del sistema como, por ejemplo: rol administrador, rol monitoreo. De cada acción ejecutada por los usuarios del sistema se debe almacenar los logs de auditoría.		
1.20	Conexiones por minuto 500.000		
1.21	Troughput (probe): 5 Gbps en total, asignado 5 Gbps en un solo appliance		
1.22	Cantidad de dispositivos a analizar: cómo mínimo 50.000		
1.23	Tipo de interfaz: Debe tener como mínimo: dos puertos (2) 10 GB cobre, dos (2) puertos 10 GB a fibra óptica (SFP+) para tráfico de Red. y un (1) puerto 1GB para Gestión (2 x 10Gbe/1Gbe - SFP+) Bypass interno sobre los puertos Gbe para garantizar la continuidad del tráfico.		
1.24	La herramienta deberá poder capturar paquetes en formato PCAPs para posteriores investigaciones forenses.		

<table>
<tr><th colspan="4">Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN</th></tr>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>CUMPLE</th><th>NO CUMPLE</th></tr>
<tr><td>1.25</td><td>La herramienta deberá permitir seleccionar las formas de visualizar las infracciones a los modelos, ya sea por usuario, dispositivo o tipos de comportamientos problemáticos.</td><td></td><td></td></tr>
<tr><td>1.26</td><td>La herramienta deberá tener la capacidad de filtrar búsquedas por fecha y hora.</td><td></td><td></td></tr>
<tr><td>1.27</td><td>La herramienta deberá permitir la generación de reportes de inteligencia de amenazas.</td><td></td><td></td></tr>
<tr><td>1.28</td><td>Toda la comunicación relacionada con la herramienta debe estar cifrada.</td><td></td><td></td></tr>
<tr><td>1.29</td><td>La herramienta debe registrar los siguientes eventos de sus usuarios:
• Alta y baja del servicio de la aplicación
• Autenticación
➢ Inicio y fin de sesión.
➢ Intentos fallidos de inicio de sesión.
➢ Bloqueo de cuentas de usuario.
• Alta, baja y modificación de usuarios.
• Alta, baja y modificación de roles
• Concesión y revocación de privilegios.
• Registro de conexiones.
• Intentos fallidos.</td><td></td><td></td></tr>
<tr><td>1.30</td><td>La herramienta como mínimo debe verificar los siguientes comportamientos y a cada uno le debe asignar una métrica:
<table>
<tr><td>1</td><td>Conexiones</td><td>26</td><td>Transferencia interna de datos (servidor)</td></tr>
<tr><td>2</td><td>Conexiones externas</td><td>27</td><td>Fallas de acceso de Kerberos</td></tr>
<tr><td>3</td><td>Conexiones internas</td><td>28</td><td>Inicio de sesión de Kerberos</td></tr>
<tr><td>4</td><td>Transferencia de datos</td><td>29</td><td>Servidores DNS externos</td></tr>
<tr><td>5</td><td>Transferencia externa de datos</td><td>30</td><td>Dominios externos que apuntan a la IP interna</td></tr>
<tr><td>6</td><td>Transferencia interna de datos</td><td>31</td><td>Paquetes externos</td></tr>
<tr><td>7</td><td>Dispositivos conectados</td><td>32</td><td>Servidores proxy externos</td></tr>
<tr><td>8</td><td>Dispositivos externos conectados</td><td>33</td><td>Alertas de FastTravel</td></tr>
<tr><td>9</td><td>Dispositivos conectados internos</td><td>34</td><td>Transferencias de archivos (EXE)</td></tr>
<tr><td>10</td><td>Conexiones activas</td><td>35</td><td>Transferencias de archivos (RAR)</td></tr>
<tr><td>11</td><td>Conexiones externas activas</td><td>36</td><td>Transferencias de archivos (binario desconocido)</td></tr>
<tr><td>12</td><td>Conexiones internas activas</td><td>37</td><td>FTP Bruteforces</td></tr>
<tr><td>13</td><td>Eventos de actividad inusuales</td><td>38</td><td>Intentos de ataque de Heartbleed</td></tr>
<tr><td>14</td><td>Transmisiones</td><td>39</td><td>Éxitos del ataque de Heartbleed</td></tr>
<tr><td>15</td><td>Solicitudes de DNS</td><td>40</td><td>Conexiones de nombre de host sin búsqueda de DNS</td></tr>
<tr><td>16</td><td>Transferencia de datos (cliente)</td><td>41</td><td>Tipos de archivos incorrectos</td></tr>
<tr><td>17</td><td>Transferencia de datos (servidor)</td><td>42</td><td>Intel APT Hits</td></tr>
<tr><td>18</td><td>Transferencia de datos externa (cliente)</td><td>43</td><td>Avisos de Inteligencia</td></tr>
</table></td><td></td><td></td></tr>
</table>

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN						
ÍTEM	DESCRIPCIÓN				CUMPLE	NO CUMPLE
	19	Transferencia de datos externa (servidor)	44	Duración de la conexión interna		
	20	Multicasts externos	45	Ratio de datos internos		
	21	Búsquedas DNS erróneas	46	Cambios en el dominio interno		
	22	Transferencia interna de datos (cliente)	47	Outputs de clúster de dispositivos		
	23	Dominios internos que apuntan a IP externa	48	Cambios en el servidor DNS		
	24	Servidores Proxy Internos	49	Avisos de paquetes abandonados		
	25	Nombres de host DNS no válidos	50	Certificados SSL no válidos		
	51	Entradas KERBEROS	78	Solicitudes DynDNS DNS		
	52	Fallo de boleto de KERBEROS	79	Solicitudes DynDNS HTTP		
	53	Enlace-Conexiones locales	80	Solicitudes DynDNS SSL		
	54	Multicasts	81	Pérdida de captura excesiva		
	55	Nuevas conexiones externas fallidas	82	Ratio de datos externos		
	56	Nuevas conexiones internas fallidas	83	Falta la notificación		
	57	Nueva conectividad interna	84	Modelos sobre-rompiendo		
	58	Éxitos de inicio de sesión POP3	85	Nuevos usos de credenciales		
	59	Sucesos de consultas de directorios SMB	86	Nuevos agentes de usuario de dispositivos		
	60	Fallas de lectura SMB	87	Nuevos dispositivos		
	61	Éxitos de lectura de SMB	88	No hay eventos de tráfico DHCP		
	62	Fallas de escritura de SMB	89	TORs salientes		
	63	Éxitos de la escritura de la PYME	90	Exploraciones de puertos		
	64	Búsquedas únicas de DNS erróneas	91	Solicitudes POST sin Get		
	65	Escaneo de direcciones	92	Cambios en el servidor proxy		
	66	Mineros Bitcoin	93	Reebots		
	67	Servidores Bitcoin Mining Pool	94	Servidores que sirven protocolos en puertos no estándar		
	68	Posibles Operaciones de Minería Bitcoin	95	Hosts bloqueados de lista de bloqueo SMTP		
	69	Casos de tráfico mal formado	96	Ambigüedades Transferidas de Datos SSH		
	70	Sistema operativo detectado	97	Contraseñas de SSH		
	71	Cambios en el clúster del dispositivo	98	SSH Ambigüedades de Transmisiones no entregadas		
	72	Errores de protocolo SSL	99	Respuestas SSL OCSP no válidas		
	73	Carga del sistema	100	Intel Match		
	74	Traceroutes	101	SSL no válidos		
	75	Usos inusuales de credenciales	102	Descargas Java		
	76	Detecciones de idiomas innusuales	103	Error al iniciar sesión en SMB		
	77	Servidores DNS internos inusuales	104	Mensaje SMB		
	105	Versiones de Software Vulnerables	112	Ataques de inyección SQL (obsoletos)		
	106	Dominios observados	113	Víctimas de inyección de SQL (obsoletas)		
	107	IPs observados	114	Detecciones de idioma inusuales		
	108	XorDetect Windows Binarios	115	Excesivas consultas NXDomain		
	109	Métricas obsoletas	116	Nombres DNS externos		
	110	Certificados APT	117	Transferencias de tipo de archivo HTTP incorrectas		
	111	Conexiones de interés				

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
1.31	No se aceptan soluciones que involucren Firewalls.		
1.32	El dispositivo a adquirir debe garantizar la integración total con los 5 appliances DARKTRACE DCIP con los que cuenta la entidad.		
1.33	La herramienta deberá contar con un módulo standalone, de contención de amenazas apoyado en inteligencia artificial, que pueda realizar bloqueos en tiempo real, tomando acciones a velocidad de máquina, mitigando las amenazas y evitando reacciones exageradas. Así mismo, este módulo y funcionalidad debe ser incluida para los cuatro (4) APPLIANCES DARKTRACE DCIP-Z y una (01) APPLIANCE DARKTRACE DCIP-M, que actualmente tiene la Policía Nacional en operación.		
1.34	La herramienta deberá ser capaz de tomar la acción a través de TCP reset sobre los appliances desplegados. No se permiten soluciones que bloqueen por medio de integraciones de terceros.		
1.35	La herramienta debe contar con 3 modos de configuración: • Pasivo • Confirmación humana • Activo / Autónomo (Selección de contención basada en Inteligencia Artificial)		
1.36	La herramienta deberá poder configurar los anteriores modos para personalizarse por hora y día de la semana.		
1.37	La herramienta deberá ser capaz de tomar los siguientes inhibidores en la red: a. Bloquear conexiones especificas maliciosas entre dispositivos internos y/o externos. b. Reforzar el comportamiento de un dispositivo. c. Reforzar el comportamiento de un grupo de dispositivos. d. Bloquear conexiones entrantes de un dispositivo. e. Bloquear conexiones salientes de un dispositivo. f. Poner en Cuarentena un dispositivo automático (La Inteligencia Artificial escogerá el mejor bloqueo a aplicar para la contención).		
1.38	La herramienta deberá contar con una ventana de visualización mostrando la siguiente información y funcionalidades: a. Panel de acciones pendientes, activas, despejadas y expiradas. b. En cada panel, debe informar el dispositivo comprometido, la acción a ejecutar o ejecutada, la duración del bloqueo y la información de los parámetros que llevan a esta acción.		
1.39	El administrador podrá tener la gestión y toma de decisión para postergar el tiempo de duración de la alerta generada por la herramienta, en caso de ser necesario.		
1.40	La herramienta deberá ser capaz de poder integrarse con los siguientes firewalls de manera activa: a. Check Point Firewall b. Cisco ASA Firewall with FirePOWER c. Cisco ASA Firewall without FirePOWER d. Cisco Firewall FirePOWER Threat Defense		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	e. FortiGate Firewall f. Palo Alto Firewall g. Juniper SRX Firewall h. F5 Big IP i. A10		
1.41	Cantidad de appliance (equipos) Mínimo uno (1), doble fuente de suministro de energía.		
1.42	El APPLIANCE se instalará y configurará en alta disponibilidad con los equipos que se encuentran actualmente instalados en la Cra 59 No. 26 -21 Oficina de Tecnologías de la Información.		
1.43	Debe renovar los (5) cinco appliances (04) DARKTRACE DCIP-Z y (01) DCIP-M, junto con el licenciamiento maching learning, que actualmente tiene la Policía Nacional, por dos (02) años.		
2	**SOPORTE**		
2.1	Mínimo dos (2) años en sitio (Cra 59 No. 26 -21 Oficina de Tecnologías de la Información), actualización de firmware y patrones de maching learning, con el cual se logra la detección durante el período que dure la garantía, el soporte deberá ser 5x8, 5 días de la semana y 8 horas diarias y deberá anexar junto con la propuesta los números de contacto para las solicitudes de soporte. Inclusive para los APPLIANCE DARKTRACE DCIP-Z y DCIP-M, con los que actualmente cuenta la Policía Nacional. Adicionalmente, el contratista debe garantizar a la institución mínimo una bolsa de 600 horas utilizables durante la vigencia del contrato. El contratista deberá presentar, a solicitud del supervisor del contrato, un reporte detallado y actualizado del consumo de horas.		
3	**GARANTÍA**		
3.1	Mínimo dos (2) años en sitio (Cra 59 No. 26 -21 Oficina de Tecnologías de la Información), en caso de daño de los APPLIANCES estos deberán ser reemplazados e instalados en un tiempo no mayor a 20 días hábiles, tiempo en el que el contratista deberá realizar las acciones pertinentes a fin de que no se presente una indisponibilidad total del servicio, inclusive para los cuatro (4) DARKTRACE DCIP-Z y un (01) DCIP-M, con los que actualmente cuenta la Policía Nacional.		
4.	**ESPECIFICACIONES TÉCNICAS PARA LA INSTALACIÓN DE EQUIPOS EN EL CENTRO DE DATOS DE LA POLICÍA NACIONAL**		
4.1	Los siguientes requerimientos técnicos deberán ser tenidos en cuenta para la instalación de servidores en el Centro de Procesamiento de Datos de la Policía Nacional ubicado en la Carrera 59 No. 26-21 CAN – Bogotá D.C., estos requerimientos podrán ser verificados en la visita técnica voluntaria. El contratista deberá conocer la topología de conexión y la disponibilidad en infraestructura suficiente para conectar los equipos, para lo cual esta será verificada mediante la visita técnica establecida en el pliego.		
4.2	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional debe ser tipo RACK en formato de 19" (*el estándar de*		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	19" se refiere a la distancia de ancho que hay entre los perfiles interiores del armario)		
4.3	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional deberá contar con doble fuente de alimentación. A su vez debe contar con la conexión de acceso no presencial en el centro de datos (Utilidad de gestión y/o administración remota)		
4.4	La infraestructura tecnológica a instalar en el centro de datos de la Policía Nacional deberá tener contrato de garantía y/o soporte vigente durante el tiempo de permanecía en el centro de datos.		
4.5	El contratista certificará los enlaces de la Fibra Óptica y cableado estructurado en cobre que sean instalados en el centro de cómputo de la Policía Nacional, como complementos necesarios para el correcto funcionamiento y conectividad de la solución tecnológica.		
4.6	Si la solución supera los requerimientos técnicos presentes en el Centro de Datos de la Policía Nacional (disponibilidad de enlaces de cobre y/o fibra óptica al igual que potencia eléctrica, para la instalación de nuevos equipos). El contratista deberá proveer además de los equipos a instalar, la infraestructura física necesaria para toda la interconexión de la solución.		
4.7	La solución de infraestructura física de cableado a instalar deberá hacerse con productos de cobre y fibra del mismo fabricante Instalado en el Centro de Datos de la Policía Nacional, para efectos de mantener la homogeneidad y compatibilidad de la solución instalada y así poder tramitar para estos nuevos enlaces la garantía dada por el fabricante que es de 25 años. Es importante también indicar que el proveedor que instale la infraestructura física de cableado en cobre y/o fibra óptica requerida sea un integrador avalado y certificado por el fabricante SIEMONS para desarrollar diseño e instalación de sus productos.		
4.8	La solución de cobre y/o fibra óptica a instalar debe ser administrable y monitoreada (solución Inteligente), por tal razón todos los elementos a instalar deben cumplir con las especificaciones técnicas.		
4.9	**PDU DE RACK O GABINETE**		
4.10	Los equipos suministrados no deberán superar la carga máxima eléctrica distribuida en cada PDU de rack o gabinete, el contratista deberá realizar las conexiones al componente eléctrico para garantizar el adecuado funcionamiento de los equipos.		
4.11	PDU Gabinetes 30Amp de mínimo 30-(C13) 6-(C19) NEMA L6-30P - Rango de temperatura de operación normal a plena carga deberá ser de mínimo 45° hasta 60° Centígrados, monitoreable de fábrica (controlador de PDU Ethernet de mínimo 10/100/1000 o 10/100 base T con IPv4 o IPv6 verticales con una capacidad mínima de carga de 4.5Kw o superior. Estas deberán ser de la misma marca y modelo de las que se encuentran instaladas actualmente en el Centro de Datos de la Policía Nacional.		
4.12	Voltaje de entrada aceptable: 200-240 VAC, Voltaje de salida: 200/240 VAC.		
4.13	Las salidas o receptáculos deben estar codificados por color, de acuerdo al grupo de receptáculos y disyuntor.		
4.14	Longitud del cable de entrada: Mínimo 3 Metros.		
4.15	Corriente máxima por salida: (C13) 10A, (C19) 16A por cada receptáculo.		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
4.16	Cantidad de interruptores automáticos internos: 2		
4.17	Tipo de disyuntor: 1 o 2 polos hidráulico-magnético		
4.18	Norma UL y/o CE (certificado europeo) y/o CSA y/o EMC, Medioambiental ROHS.		
4.19	Las Pdu de Rack deben tener una capacidad de distribución de poder bifásica y deberán ser energizadas por el contratista en su totalidad hacia los tableros de distribución. Las PDU deberán poderse comunicar a través de los protocolos SNMP y proveer los archivos de los MIB'S que permitan la lectura de los diferentes parámetros de monitoreo de cada una de las PDU para integrarse con las herramientas de monitoreo de la Policía Nacional.		
4.20	La PDU monitoreables deberán ser configuradas para el monitoreo de las siguientes variables de consumo: • Potencia • Voltaje • Corriente • Kilovatios por hora • Factor de Potencia • Frecuencia • KVA		
4.21	**SOLUCIÓN DE COBRE CABLE UTP EN CATEGORIA 6A**		
4.22	Debe cumplir o superar las especificaciones de la norma ANSI/TIA-568-2-D, el estándar IEEE 802.3an-2006 de requerimientos de canal para soportar 10GBASE-T.		
4.23	Deberá soportar por lo menos las siguientes aplicaciones: 100 Mb/s Ethernet 10GBase-T, 100Base-TX (Fast Ethernet), 1000base-T (Gigabit Ethernet); IEEE 802.3, ANSI X3.263; 1.2Gb/s ATM; Token Ring 4/16 para Voz y Datos.		
4.24	Deberá existir compatibilidad mecánica y eléctrica de los productos y cables de la Categoría 6A, con las categorías anteriores.		
4.25	El forro debe ser continuo, sin porosidades u otras imperfecciones, con especificación de su cubierta o chaqueta type LSZH (UL o ETL) de acuerdo a la norma IEC 60332-3. Retardante de llama, no generar gas toxico y libre de halógenos (LSZH).		
4.26	El cable deberá ser de construcción tubular en su apariencia externa (redondo). Dentro del cable, los conductores de cobre deben estar trenzados en pares firmemente y estos deben tener separación individual para mejorar su desempeño. El cable deberá ser calibre No. 23 AWG, debe ser elaborado por el mismo fabricante de la conectividad y estar probados por laboratorio ETL para Categoría 6A respectivamente.		
4.27	Los enlaces con cables de cobre deberán ser de 4 pares trenzados sólidos, del tipo F/UTP (blindado). La conexión final a los patch panels correspondientes se deberá hacer con el método de conexión T568B.		
4.28	No se aceptarán cables con conductores pegados u otros métodos de ensamblaje que requieran herramientas especiales para su terminación.		
4.29	Deberá poseer un elemento que ayude a reducir los efectos de alíen Cross Talk		
4.30	El forro del cable debe ser color azul y tener impresa, como mínimo, la siguiente información: nombre del fabricante, número de parte, tipo de		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	cable, número de pares, tipo de listado (LSZH), y las marcas de mediciones secuenciales para verificación visual de longitudes.		
4.31	El cable deberá permitir en su instalación al menos un radio mínimo de curvatura de 4 veces su diámetro externo a una temperatura de 0ºC sin ocasionar deterioro en forro o aislantes.		
4.32	Velocidad de propagación >69% de 10 a 500 Mhz, Debe poseer una impedancia característica de 100Ω, +/- 15% hasta 100Mhz, +/- 22% entre 100 – 350Mhz y +/- 32% entre 350 – 500Mhz de respuesta para ancho de banda de acuerdo con el ANSI/TIA 568-2-D para categoría 6 A.		
4.33	Debe cumplir con IEEE 802.3af, IEEE 802.3at y los requerimientos de 802.3bt		
4.34	La clasificación de flamabilidad de la chaqueta debe cumplir con IEC 60332-3, 60754-2, 61034-2		
4.35	Para la instalación de los enlaces de cobre en los EDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels ZMAX, Empty, Shielded, 48 Openings, Angled, 1U, Black, Fixed Wire Manager, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional		
4.36	Para la instalación de los enlaces de cobre en los HDA´s (Patch panels modulares angulados) se deberán utilizar herrajes de patch panels inteligentes del tipo MapIT, Empty, Shielded, 24 Openings, Angle, 1U, Black, Fixed Wire Manager, Keystone, Referencia Siemon: M-SPPA-K24ENS, los cuales deberán estar conectados a un panel de control maestro MapIT, 24 Port, 1U, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional. Es importante que el proveedor verifique si existe disponibilidad de puertos de conexión en el panel de control maestro, en caso de que no haya disponibilidad será necesario instalar un panel de control maestro adicional.		
4.37	Para los herrajes de patch panel del sistema inteligente ubicados en los HDA´s los cables de cobre deberán ser instalados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Keystone, Black, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.38	Para los herrajes de patch panel ubicados en los EDA´s los cables de cobre deberán ser terminados en tomas o jacks RJ-45 ZMAX, Shielded, Category 6A, RJ45, Panel Mount, Tool-Less, T568A/B, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.39	Para la habilitación de los servicios en los EDA´s será necesario utilizar patch cords RJ45 a RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack. Para la habilitación de los servicios en los HDA´s será necesario utilizar patch cords del sistema inteligente MapIT, RJ45 a RJ45, Category 6A, U/FTP, T568A/B, Stranded, LSOH-1, Blue Cable, Blue Boot, 2 Meters, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.40	Todos los componentes de cobre (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	un equipo de certificación avalado por el fabricante del cableado de cobre, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas se deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
4.41	Para la conexión de COBRE ADMINISTRACION se requiere que el contratista instale: Copper, Patch Cord, RJ45, RJ45, Category 6A, S/FTP, T568A/B, Stranded, CM/LSOH-1, White Cable, Clear Boot, 7 Feet, Bulk Pack,3 Meter, No. parte ZM6A-S07-06B 19SIZM6AS0706B , Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
4.42	**SOLUCIÓN DE FIBRA OPTICA**		
4.43	Los enlaces con cables de fibra óptica pre-conectorizados deberán ser MTP/MTP de 12 hilos, del tipo multimodo OM4, y velocidades de hasta 10 Gbseg hasta 550 metros sobre enlaces dúplex (2 hilos) o velocidades de hasta 40 Gbseg sobre 4 enlaces dúplex (8 hilos).		
4.44	Estos cables de fibra deben ser Plug & Play, Trunk, 12 Strand, RazorCore, XGLO, Multimode, Female MTP Base 12 Solution, Female MTP Base 12 Solution, Polarity C, OM4, 50/125, Aqua, LSOH-3C, Pulling Eye, XX Meter, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional donde XX corresponde a la distancia en metros.		
4.45	Para la conexión de los enlaces de fibra óptica en los HDA´s 3 (Bandeja de alta densidad) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo LightStack, Rack Mount, 1U, Sliding Access, 12 Openings, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.46	Para la conexión de los enlaces de fibra óptica en los EDA´s (Bandeja de conexión) se deberán utilizar bandejas de fibra óptica u ODF´s del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC, MTP, OM4, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.47	Como el sistema de fibra óptica es inteligente y está característica se realiza en los gabinetes EDA's bajo una topología de cross conexión se deben utilizar también bandejas u ODF´s (Bandeja de Cross conexión) de fibra óptica del tipo inteligente MapIT, G2 Smart, Enclosure, 1U, Multimode, 48 Fiber, Aqua, LC a LC, OM4, Black, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.48	Para la adecuada conexión de los cables de fibra óptica MTP/MTP a las bandejas de fibra óptica u ODF´s (Cassettes pre conectorizados) es requerido que estos cables sean conectados a cassettes pre conectorizados del tipo MTP a 6 LC dúplex, OM4, multimodo, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.49	Para la conexión de equipos en los EDA´s y HDA´s se deberán utilizar patch cords entre las bandejas inteligentes de cross conexión de los EDA´s a los puertos de los equipos y las bandejas de alta densidad a los puertos de los switches de fibra en los HDA´s, estos patch cords deberán ser dúplex, XGLO, Multimode, LC BladePatch a LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 2 Meter, de la misma		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.50	Adicionalmente, como la topología de conexión en los EDA´s es de cross conexión y el sistema es inteligente, es requerido utilizar patch cords dúplex del tipo inteligentes entre la bandeja que recibe los cables troncales de fibra MTP/MTP en cassettes pre conectorizados y la bandeja de cross conexión que habilita los servicios de los equipos, estos patch cords deben ser del tipo MapIT, Duplex, XGLO, Multimode, LC a LC, OM4, 50/125, Aqua, OFNR, 1 Meter, de la misma marca del fabricante instalado en el centro de datos de la Policía Nacional.		
4.51	En caso de instalar enlaces nuevos de fibra óptica el contratista deberá verificar si hay disponibilidad de espacio en las bandejas de alta densidad de los HDA´s, en las bandejas inteligentes de los EDA´s, y en las bandejas inteligentes de cross conexión de los EDA´s, en caso de no tener disponibilidad deberán instalar bandejas nuevas con las especificaciones técnicas anteriormente descritas.		
4.52	Todos los componentes de fibra óptica (cables y conectividad) que se instalen nuevos deberán ser debidamente identificados y marquillados cumpliendo las normas ANSI/TIA-606-C, y deberán ser probados con un equipo de certificación avalado por el fabricante del cableado de cobre, y este a su vez deberá contar con certificado de calibración vigente expedido por el fabricante del equipo, las pruebas deberán hacerse para enlace permanente y cumpliendo con los límites de medición de la ISO 11801.		
4.53	Para la conexión de FIBRA SAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Erika Violet, LSOH-3C, 3 Meter. No. Parte FBP-LCLC5V-02EH o 19SIFBPLCLC5V02EH, Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
4.54	Para la conexión de FIBRA LAN, se requiere que el contratista instale: Fiber, Jumper, Duplex, XGLO, Multimode, LC BladePatch, LC BladePatch, RFP, OM4, 50/125, Aqua, LSOH-3C, 3 Meter. No. parte FBP-LCLC5V-02AH 19SIFBPLCLC5V02AH. Marca Siemon. Que sean necesarios para la conexión total de los puertos del equipamiento tecnológico.		
5	**EXPERIENCIA DEL PERSONAL**		
5.1	Se requiere mínimo de una (01) persona quien debe acreditar estudios en ingeniería de sistemas y/o electrónica y/o afines, con capacitación en la herramienta y experiencia mínima de un (1) año en instalación y puesta en funcionamiento de herramientas similares al del presente contrato. Para lo cual, el oferente deberá presentar con la propuesta, la tarjeta profesional de la persona en alguna de las ingenierías solicitadas, una (01) certificación que evidencie el manejo de la herramienta por parte del fabricante y una (01) certificación en el manejo de la plataforma de red ofertada o herramienta de análisis comportamental en la WAN, donde se evidencie experiencia mínima de un año en instalación y puesta en funcionamiento de herramientas de análisis comportamental o similares al objeto del presente proceso.		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
6	**TRANSFERENCIA DE CONOCIMIENTO**		
6.1	Se deberá brindar transferencia de conocimiento certificada por el fabricante para diez (10) funcionarios en las instalaciones de la Oficina de Tecnologías de la Información, en los siguientes roles: administración, manejo y análisis de la información entregada por la herramienta Esta capacitación deberá tener una intensidad horaria mínima de cuarenta (40) horas hábiles y certificada por la empresa fabricante.		
7	**DERECHOS DE AUTOR**		
7.1	En atención al numeral 15 del capítulo IX “Parámetros y recomendaciones adicionales que orientan el cumplimiento del régimen jurídico del derecho de autor y los derechos conexos de la Circular conjunta No. 004 del 24/04/2006 de la Procuraduría General de la Nación y la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor, el proponente deberá presentar con la oferta una certificación de distribuidor autorizado o certificado de autenticidad y certificado de registro de soporte lógico – software, expedido por la Dirección Nacional de derechos de autor.		
7.2	El contratista deberá entregar un certificado de Fabricante donde se evidencie la autenticidad del software contratado con vigencia máxima de 30 días y relacionándose al proceso en mención.		
8	**COMPONENTE AMBIENTAL**		
8.1	El oferente deberá presentar el certificado de consulta del Registro Único de Infractores Ambientales (RUIA), expedido a través del enlace oficial del Ministerio de Ambiente: https://vital.minambiente.gov.co/SILPA_UT_PRE/RUIA/ConsultarSancion.aspx?Ubic=ext.,; En caso de presentarse como unión temporal o consorcio, deberá aportarse el certificado RUIA de cada uno de sus integrantes. Así mismo, este certificado deberá ser presentado durante la ejecución del contrato cuando el supervisor lo requiera, con el fin de verificar la existencia o no de sanciones ambientales vigentes.		
8.2	El oferente deberá verificar la necesidad de permisos, licencias, concesiones o autorizaciones ambientales de acuerdo a su actividad comercial y, de ser legalmente exigibles, obtenerlos y presentar el documento emitido por la autoridad ambiental competente. En caso de que no aplique deberá declararlo el representante legal bajo la gravedad de juramento, asumiendo plenamente las consecuencias legales, ambientales y contractuales que se deriven del incumplimiento. Se deberán mantener vigentes durante toda la ejecución del contrato.		
9	**ACUERDO DE CONFIDENCIALIDAD**		
9.1	Si la Policía Nacional considera pertinente someter a estudio de seguridad al contratista, éste permitirá y facilitará todos los medios que la Entidad le solicite para este fin. El Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del contrato y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	tenga acceso con ocasión de su servicio y sea revelada información marcada como confidencial. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información, para lo cual deberá diligenciar el formulario "ACUERDO DE CONFIDENCIALIDAD".		
10	**COMPROMISO ANTICORRUPCIÓN.**		
10.1	Cumplir con el compromiso de anticorrupción durante la ejecución del contrato, manifestando que se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del contratista, sus empleados, representantes, asesores o de cualquier otra persona que actúe en su nombre, es causal suficiente para la terminación anticipada del contrato, para lo cual el oferente deberá diligenciar y entregar con la oferta el formulario "COMPROMISO ANTICORRUPCIÓN".		
11	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO.**		
11.1	El contratista deberá cumplir con la implementación del sistema de Gestión de Seguridad y Salud en el Trabajo, para lo cual deberá diligenciar el formulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO".		
11.2	El oferente deberá acreditar el cumplimiento de los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), en los términos establecidos por el Decreto 1072 de 2015 y por la Resolución 0312 de 2019 del Ministerio del Trabajo, mediante la presentación de la calificación oficial radicada ante la Administradora de Riesgos Laborales ARL y/o ante el Ministerio del Trabajo de conformidad con la circular 027 de 2026, correspondiente al año inmediatamente anterior a la fecha de cierre del presente proceso de selección.		
11.3	El contratista debe acreditar, mediante los soportes documentales pertinentes, el cumplimiento de las obligaciones legales relacionadas con el pago de los aportes al Sistema de Seguridad Social Integral, prestaciones sociales y afiliación y pago a la Administradora de Riesgos Laborales ARL de sus trabajadores en misión al objeto contractual.		
12	**EXPERIENCIA DEL PROPONENTE**		
12.1	**EXPERIENCIA GENERAL PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL O REPRESENTACIÓN EN COLOMBIA -RUP** El Registro Único de Proponentes es el instrumento a través del cual se verificará el requisito de experiencia del proponente, para tal efecto las personas naturales, las personas jurídicas, las uniones temporales, los consorcios u otra forma de asociación que participen en este proceso, deberán acreditar la experiencia con mínimo uno (01) máximo tres (03) contratos celebrados y ejecutados con entidades públicas y/o privadas, identificados con alguno de los siguientes códigos UNSPSC y que su valor sumado sea igual o superior a 856,69 SMMLV, así:		

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
432332	Difusión de Tecnologías de información y	Software	Software de seguridad y protección	856,69

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	<table><tr><td></td><td>telecomunica-ciones</td><td></td><td></td><td></td></tr></table> **NOTA 1:** si los contratos acreditados fueron realizados bajo la modalidad de Consorcio, de Unión Temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio, de la Unión Temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio, la Unión Temporal u otras formas de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato. **NOTA 2:** en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP con alguno de los códigos UNSPSC antes señalados. **NOTA 3**: en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario **"EXPERIENCIA GENERAL DEL PROPONENTE**", donde relacionará los contratos para la evaluación. **EXPERIENCIA ESPECÍFICA PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL EN COLOMBIA** El proponente que vaya a proveer los bienes o servicios objeto del presente proceso de contratación, trátese de personal natural o jurídica, deberá anexar mínimo una (01) máximo tres (03) constancias (certificaciones o actas de liquidación) de contratos celebrados y ejecutados con entidades públicas y/o privadas, cuyo objeto sea igual o similar al objeto de la presente contratación "HERRAMIENTA DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LA RED" o relacionados con seguridad de APIS, documentos que como mínimo deberán tener la siguiente información: 1. Nombre del contratista 2. Nombre del contratante 3. Objeto del contrato 4. Valor del contrato 5. Fecha de suscripción y fecha de inicio del contrato 6. Fecha de terminación del contrato 7. Personal de contacto para verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). 8. Estado del contrato: ejecutado o liquidado. 9. Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. 10. Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. 11. Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otra forma de asociación.		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	NOTA 1: en cumplimiento del artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, el Decreto 1860 de 2021 el cual reglamentó parcialmente la Ley 2069 de 2020 "Por medio de la cual se impulsa el emprendimiento en Colombia" y el artículo 1º del Decreto 0287 de 2026 "Por el cual se modifican los artículos 2.2.1.2.4.2.6., 2.2.1.2.4.2.7. y 2.2.1.2.4.2.8. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación", se toma como criterio diferencial para las MiPymes y los emprendimientos y empresas de personas con discapacidad, el número de contratos para la acreditación de la experiencia. Por tanto, deberán anexar mínimo una (01) máximo cuatro (04) constancias (certificaciones o actas de liquidación) que cumplan con lo antes relacionado. **NOTA 2:** la experiencia específica presentada deberá estar registrada en el Registro Único de Proponentes, no serán tenidas en cuenta aquellas constancias de contratos que no se encuentren registrados. **NOTA 3:** si la información relacionada en el (RUP) para acreditar la experiencia no se puede verificar**,** la entidad se reserva la facultad de solicitar información adicional. **NOTA 4**: no se aceptarán auto certificaciones. **NOTA 5**: no se tendrán en cuenta las certificaciones de contratos en ejecución. **NOTA 6:** no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas. **NOTA 7:** cuando los documentos no indiquen su valor en SMMLV o si estos son de años anteriores a 2026, se hará la respectiva conversión de acuerdo al año en que terminó el contrato. La verificación será realizada por el comité evaluador técnico. **NOTA 8:** si los contratos acreditados fueron realizados bajo la modalidad de consorcio, unión temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del consorcio, unión temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del consorcio, unión temporal u otra forma de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes en la ejecución del contrato. **NOTA 9:** en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP según el código UNSPSC requerido en el presente proceso de selección. **NOTA 10**: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo		

Lote 3: HERRAMIENTA DE ANALISIS COMPORTAMENTAL EN LA WAN			
ÍTEM	**DESCRIPCIÓN**	**CUMPLE**	**NO CUMPLE**
	proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite. La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma. **NOTA 11:** en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario “EXPERIENCIA DEL PROPONENTE”, donde relacionará los contratos para la evaluación. La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.		