FICHA TÉCNICA DE PRODUCTO

DENOMINACIÓN DE BIEN O SERVICIO
HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
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 el envío de alertas, estas deben ser cambiantes de acuerdo a la probabilidad de que el comportamiento del usuario esté fuera de los rangos normales. Auto aprendizaje basado en algoritmos de machine learning no supervisado, debe iterar constantemente la verificación del uso normal de la red. Adicional a esto, la solución 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. 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)

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
	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. 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 por 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	La herramienta deberá poder capturar paquetes en formato PCAPs para posteriores investigaciones forenses.
1.21	La herramienta deberá permitir seleccionar las formas de visualizar las infracciones a los modelos, ya sea por usuario, dispositivo o tipos de comportamientos problemáticos.
1.22	La herramienta deberá tener la capacidad de filtrar búsquedas por fecha y hora.
1.23	La herramienta deberá permitir la generación de reportes de inteligencia de amenazas.
1.24	Toda la comunicación relacionada con la herramienta debe estar cifrada.
1.25	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.

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
1.26	La herramienta como mínimo debe verificar los siguientes comportamientos y a cada uno le debe asignar una métrica:

1	Conexiones	26	Transferencia interna de datos (servidor)
2	Conexiones externas	27	Fallas de acceso de Kerberos
3	Conexiones internas	28	Inicio de sesión de Kerberos
4	Transferencia de datos	29	Servidores DNS externos
5	Transferencia externa de datos	30	Dominios externos que apuntan a la IP interna
6	Transferencia interna de datos	31	Paquetes externos
7	Dispositivos conectados	32	Servidores proxy externos
8	Dispositivos externos conectados	33	Alertas de FastTravel
9	Dispositivos conectados internos	34	Transferencias de archivos (EXE)
10	Conexiones activas	35	Transferencias de archivos (RAR)
11	Conexiones externas activas	36	Transferencias de archivos (binario desconocido)
12	Conexiones internas activas	37	FTP Bruteforces
13	Eventos de actividad inusuales	38	Intentos de ataque de Heartbleed
14	Transmisiones	39	Exitos del ataque de Heartbleed
15	Solicitudes de DNS	40	Conexiones de nombre de host sin búsqueda de DNS
16	Transferencia de datos (cliente)	41	Tipos de archivos incorrectos
17	Transferencia de datos (servidor)	42	Intel APT Hits
18	Transferencia de datos externa (cliente)	43	Avisos de Inteligencia
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	Exitos 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

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
	<table><tr><td>61</td><td>Exitos de lectura de SMB</td><td>88</td><td>No hay eventos de tráfico DHCP</td></tr><tr><td>62</td><td>Fallas de escritura de SMB</td><td>89</td><td>TORs salientes</td></tr><tr><td>63</td><td>Exitos de la escritura de la PYME</td><td>90</td><td>Exploraciones de puertos</td></tr><tr><td>64</td><td>Búsquedas únicas de DNS erróneas</td><td>91</td><td>Solicitudes POST sin Get</td></tr><tr><td>65</td><td>Escaneo de direcciones</td><td>92</td><td>Cambios en el servidor proxy</td></tr><tr><td>66</td><td>Mineros Bitcoin</td><td>93</td><td>Reebots</td></tr><tr><td>67</td><td>Servidores Bitcoin Mining Pool</td><td>94</td><td>Servidores que sirven protocolos en puertos no estándar</td></tr><tr><td>68</td><td>Posibles Operaciones de Minería Bitcoin</td><td>95</td><td>Hosts bloqueados de lista de bloqueo SMTP</td></tr><tr><td>69</td><td>Casos de tráfico mal formado</td><td>96</td><td>Ambigüedades Transferidas de Datos SSH</td></tr><tr><td>70</td><td>Sistema operativo detectado</td><td>97</td><td>Contraseñas de SSH</td></tr><tr><td>71</td><td>Cambios en el clúster del dispositivo</td><td>98</td><td>SSH Ambigüedades de Transmisiones no entregadas</td></tr><tr><td>72</td><td>Errores de protocolo SSL</td><td>99</td><td>Respuestas SSL OCSP no válidas</td></tr><tr><td>73</td><td>Carga del sistema</td><td>100</td><td>Intel Match</td></tr><tr><td>74</td><td>Traceroutes</td><td>101</td><td>SSL no válidos</td></tr><tr><td>75</td><td>Usos inusuales de credenciales</td><td>102</td><td>Descargas Java</td></tr><tr><td>76</td><td>Detecciones de idiomas innusuales</td><td>103</td><td>Error al iniciar sesión en SMB</td></tr><tr><td>77</td><td>Servidores DNS internos inusuales</td><td>104</td><td>Mensaje SMB</td></tr><tr><td>105</td><td>Versiones de Software Vulnerables</td><td>112</td><td>Ataques de inyección SQL (obsoletos)</td></tr><tr><td>106</td><td>Dominios observados</td><td>113</td><td>Víctimas de inyección de SQL (obsoletas)</td></tr><tr><td>107</td><td>IPs observados</td><td>114</td><td>Detecciones de idioma inusuales</td></tr><tr><td>108</td><td>XorDetect Windows Binarios</td><td>115</td><td>Excesivas consultas NXDomain</td></tr><tr><td>109</td><td>Métricas obsoletas</td><td>116</td><td>Nombres DNS externos</td></tr><tr><td>110</td><td>Certificados APT</td><td>117</td><td>Transferencias de tipo de archivo HTTP incorrectas</td></tr><tr><td>111</td><td>Conexiones de interés</td><td></td><td></td></tr></table>
1.27	No se aceptan soluciones que involucren Firewalls.
1.28	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.
1.29	La herramienta debe contar con 3 modos de configuración: • Pasivo • Confirmación humana • Activo / Autónomo (Selección de contención basada en Inteligencia Artificial)
1.30	La herramienta deberá poder configurar los anteriores modos para personalizarse por hora y día de la semana.
1.31	La herramienta deberá ser capaz de tomar los siguientes inhibidores en la red: a. Bloquear conexiones específicas 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, teniendo en cuenta lo establecido en el ítem 1.35).

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
1.32	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.
1.33	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.
1.34	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 e. FortiGate Firewall f. Palo Alto Firewall g. Juniper SRX Firewall h. F5 Big IP i. A10 Nota: se relacionan las marcas con las que la Institución cuenta actualmente.
1.35	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.
1.36	El oferente deberá tener en cuenta que, en la actualidad, la Policía Nacional cuenta con una solución de análisis comportamental para la red WAN de marca Darktrace, compuesta por cinco (5) dispositivos tipo appliance, distribuidos en cuatro (4) unidades DARKTRACE DCIP-Z y una (1) unidad DARKTRACE DCIP-M. Por lo anterior, el oferente deberá contemplar dentro de su propuesta la renovación del soporte, mantenimiento y licenciamiento asociado de los cinco (5) dispositivos existentes por el tiempo de garantía (2 años). Adicionalmente, deberá incluir la provisión e implementación de un (1) nuevo dispositivo tipo appliance con doble fuente de suministro de energía que se integre con la solución actual y que cumpla integralmente con los requerimientos técnicos establecidos en el presente proceso y con los siguientes parámetros: -Conexiones por minuto: mínimo 500.000 -Troughput (probe): mínimo 5 Gbps en total, asignado 5 Gbps en un solo appliance. -Cantidad de dispositivos a analizar: cómo mínimo 50.000 -Tipo de interfaz: Debe tener como mínimo: dos puertos (2) 10 GB cobre, dos (2) puertos 10 GB a fibra óptica (1Gbe/10Gbe SFP+) para tráfico de Red. y un (1) puerto 1GB para Gestión, cables y conectores requeridos para el funcionamiento. Bypass interno sobre los puertos Gbe para garantizar la continuidad del tráfico.
1.37	La solución deberá ser instalada y configurada en alta disponibilidad en la Cra 59 No. 26 -21 en el datacenter de la Policía Nacional a cargo de la Oficina de Tecnologías de la Información.
1.38	El oferente deberá contar con disponibilidad y stock de los componentes requeridos, de manera que pueda garantizar el cumplimiento del plazo de ejecución establecido para el presente proceso. Para tal efecto, deberá anexar junto con su oferta una certificación suscrita por el representante legal, mediante la cual manifieste y certifique que cuenta con la disponibilidad de los elementos, componentes y demás recursos necesarios para llevar a cabo la implementación objeto del presente proceso dentro del plazo establecido.

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
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. Adicionalmente, el contratista debe garantizar a la Institución mínimo una bolsa de 600 horas utilizables durante la vigencia del contrato, a partir del recibo a satisfacción. 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 de garantía en sitio, en la dirección Cra. 59 No. 26-21, Oficina de Tecnologías de la Información. En caso de falla de alguno de los equipos de la solución, deberá ser reemplazado e instalado en un plazo no mayor a veinte (20) días hábiles, durante el cual el contratista deberá ejecutar las acciones necesarias para evitar la indisponibilidad total del servicio. Lo anterior, no generará costo adicional para la Policía Nacional de Colombia. Esta iniciará a partir del recibo a satisfacción de la solución.
3.2	En caso de que alguno de los equipos presente degradación en el desempeño o en la calidad del servicio, deberá ser reemplazado bajo garantía, sin costo adicional para la Policía Nacional de Colombia. Para tal efecto, se realizarán validaciones conjuntas entre el contratista y el fabricante, con el fin de determinar si la afectación obedece a limitaciones de desempeño del equipo frente a los requerimientos de la solución ofertada, procediendo, en caso afirmativo, con el respectivo cambio en garantía.
3.3	El proponente deberá acreditar que es partner vigente del fabricante de la solución ofertada para el año de la presente contratación. Para ello, deberá anexar una carta o certificación oficial emitida por el fabricante, en la cual se indique expresamente que el proponente cuenta con la calidad de partner autorizado y vigente para la comercialización, implementación y/o soporte de la solución ofrecida. Esta certificación deberá contar con datos de contacto de Colombia para verificación.
3.4	El oferente deberá garantizar que la solución ofertada cuenta con soporte técnico oficial del fabricante y acceso a actualizaciones de software y firmware si es el caso, durante el período mínimo de garantía.
3.5	Los componentes ofertados, no deberán estar próximos a su fin de ciclo de vida (End of Life - EOL) ni a su fin de soporte (End of Support - EOS) según la política del fabricante. El contratista deberá garantizar que los productos cuentan con soporte oficial durante el período mínimo de garantía.
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 por parte del Contratista 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.
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 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.

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
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.
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

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
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 tóxico 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 alien 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 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 0°C 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.

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
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 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 ADMINISTRACIÓN 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 ÓPTICA**
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 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

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
	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 o electrónica, experiencia mínima de un (1) año en instalación y puesta en funcionamiento de la solución ofertada objeto del presente proceso. Para lo cual, el oferente deberá presentar con la propuesta, la siguiente documentación: - Hoja de vida - Diploma - Tarjeta profesional vigente de alguna de las ingenierías solicitadas (mínimo 2 años de experiencia a partir de la expedición de la tarjeta profesional) - Una (01) certificación que evidencie el manejo e implementación de la herramienta por parte del fabricante. - Una (01) certificación en el manejo e implementación de la solución ofertada de herramienta de análisis comportamental en la WAN, donde se evidencie experiencia mínima de un (1) año en instalación y puesta en funcionamiento de la misma.
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

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
	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	La Policía Nacional realizará la 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, se consultará de cada uno de sus integrantes.
8.2	El oferente deberá verificar si, para el funcionamiento de su actividad comercial, se requieren permisos, licencias, concesiones o demás autorizaciones de carácter ambiental y, en caso de ser legalmente exigibles, deberá obtenerlos y presentar junto con su oferta el documento expedido por la autoridad ambiental competente. En caso de que dichos permisos, licencias, concesiones o autorizaciones no se requieran para el funcionamiento de su actividad comercial, el representante legal deberá indicarlo expresamente bajo la gravedad de juramento al momento de presentar la oferta, manifestando que su actividad no está sujeta a este tipo de exigencias, y asumiendo las consecuencias legales, ambientales y contractuales derivadas de la información suministrada.
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 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 oferente deberá acreditar el cumplimiento de los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), conforme a lo establecido en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 del Ministerio del Trabajo. Para tal efecto, deberá presentar la calificación oficial de los Estándares Mínimos correspondiente al cierre del año inmediatamente anterior, la cual podrá ser acreditada mediante

HERRAMIENTA DE ANÁLISIS COMPORTAMENTAL EN LA WAN	
ÍTEM	**DESCRIPCIÓN**
	cualquiera de las siguientes alternativas, ambas válidas conforme a la normativa vigente y a la Circular 027 de 2026: • Calificación de la autoevaluación de los estándares mínimos radicada ante la Administradora de Riesgos Laborales (ARL), ó • Calificación de la autoevaluación de los estándares mínimos radicada ante el Ministerio del Trabajo. (plazo establecido hasta el 31 de julio de 2026 conforme a los establecido en la circular 027 de 2026) **Nota:** Este requisito deberá entregarlo junto con la oferta. • Los proponentes extranjeros que no tengan sucursal en Colombia estarán exceptuados de la obligación de presentar esta información, debe declararlo bajo una declaración juramentada indicando esta condición y entregar al supervisor del contrato en cumplimiento de este criterio. • Para personas naturales sin personal a cargo, no será exigible este requisito, debe declararlo bajo una declaración juramentada indicando esta condición y entregar al supervisor del contrato en cumplimiento de este criterio.

Subintendente **JOJAN DANIEL PRADO FULA**
Estructurador Estudio Previo

Intendente **JAIRO ALEXANDER ESTUPIÑAN ALVARADO**
Estructurador Estudio Previo

Intendente Jefe **CESAR ARMANDO RUÍZ QUIÑONEZ**
Estructurador Estudio Previo

Intendente Jefe **DIEGO FERNANDO PINTO PRADA**
Estructurador Estudio Previo