ANEXO ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO

Facatativá XX de XXXXX de 2026

(El apoderado o representante legal), obrando en nombre y representación de conformidad con lo establecido en la Invitación a ofertar, ofertó de forma irrevocable, los siguientes bienes o servicios objeto del presente proceso de contratación, con las siguientes características técnicas:

Para efectos de establecer las especificaciones técnicas del presente proceso, se dará aplicación a las especificaciones técnicas "**APPLIANCES PARA EL MONITOREO Y ANÁLISIS DE TRÁFICO DE RED"** y las **ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO** con radicado No. 2026574008246773: MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI–EJE-CP-B., de fecha 16 de marzo de 2026, las cuales contienen los parámetros técnicos que deben cumplir los oferentes en la acreditación del servicio, así mismo, el contenido es el mismo del **ANEXO ESPECIFICACIONES TÉCNICAS**, los cuales se describen a continuación:

APPLIANCES PARA EL MONITOREO Y ANÁLISIS DE TRÁFICO DE RED			
SUBSISTEMA: Comunicaciones			
ESPECIALIDAD: Comunicaciones			
PROCESO: Gestión de tecnologías y sistemas de información C5		**NIVEL DE CLASIFICACIÓN:** Público	
Código ET: ET-JEMPP-CEDE6-0562	**Versión:** 0	**Fecha de emisión:** 2026-03-02	**Número de Páginas:** 38

Elaboró	Revisó	Aprobó
SV. PRADO ESCOBAR LUIS EDUARDO Analista de Seguridad Cibernética CS. ARANGO CARVAJAL VALERIA Analista de Seguridad Cibernética	PS. ALEJANDRA BETANCOURTH Asesora Jurídica CEDE6 CT. JINNA MARCELA DEVIA PÉREZ Oficial de Planificación y Políticas MY. FREDY MAURICIO RUIZ GUTIERREZ Ejecutivo y Segundo Comandante BACCI TC. ROGER JESÚS BUELVAS NÁRVAEZ Comandante del BACCI	CR. EDWARD ENRIQUE ARÉVALO RIOS Comandante de la Brigada de Interoperabilidad Computación y Ciberdefensa

1 OBJETO

La presente Especificación Técnica tiene por objeto definir los parámetros funcionales, operativos y de interoperabilidad para la adquisición, instalación, configuración, integración y puesta en operación de appliances especializados para el monitoreo y análisis avanzado de tráfico de red, el cual deberá ser compatible con la solución de protección NDR (Network Detection and Response) destinados a la protección de la infraestructura de red del Ejército Nacional, con el propósito de fortalecer el monitoreo integral del tráfico y potenciar las capacidades de detección autónoma de amenazas detectadas en la red del Ejército Nacional, a fin de asegurar su correcto funcionamiento.

El objeto comprende la incorporación de estos dispositivos dentro de la arquitectura de red institucional, con el propósito de:

- Incrementar la visibilidad integral del tráfico en los diferentes segmentos de la infraestructura de comunicaciones.
- Potenciar las capacidades de detección autónoma de amenazas y análisis de comportamiento anómalo.
- Fortalecer la capacidad de monitoreo continuo y respuesta oportuna frente a incidentes cibernéticos.
- Garantizar la protección, integridad y disponibilidad de los activos de información críticos para la misión institucional.

En consecuencia, la implementación de los appliances deberá contribuir al robustecimiento de la postura defensiva del Ejército Nacional en el dominio ciber, asegurando un funcionamiento eficiente, confiable y alineado con los estándares técnicos de seguridad en redes de carácter estratégico y militar.

2 DEFINICIONES, CLASIFICACIÓN Y APLICACIÓN

2.1 DEFINICIONES

ACL (Lista de Control de Acceso). Una lista de control de acceso a la red (ACL) está compuesta por reglas que permiten el acceso a un entorno informático o lo rechazan. De alguna manera, una ACL es como una lista de invitados en un club exclusivo. Solo las personas de la lista están permitidas en las puertas. Esto permite a los administradores garantizar que, a menos que el dispositivo presente las credenciales adecuadas, no pueda obtener acceso.

AI (Inteligencia Artificial). La inteligencia artificial (IA) es una tecnología que permite a las computadoras y máquinas simular el aprendizaje humano, la comprensión, la resolución de problemas, la toma de decisiones, la creatividad y la autonomía.

AWS (Servicios Web de Amazon). Amazon Web Services (AWS) es la nube más adoptada y completa en el mundo, que ofrece más de 200 servicios integrales de centros de datos a nivel global. Millones de clientes, incluso las empresas emergentes que crecen más rápido, las compañías más grandes y los organismos gubernamentales líderes, están usando AWS para reducir los costos, aumentar su agilidad e innovar de forma más rápida.

CPM (Conexiones Por Minuto) RTT. El tiempo de ida y vuelta (RTT) en redes es el tiempo que se tarda en obtener una respuesta después de iniciar una solicitud de red. Cuando interactúa con una aplicación, por ejemplo, al hacer clic en un botón, la aplicación envía una solicitud a un servidor de datos remoto. A continuación, recibe una respuesta de datos y le muestra la información. El RTT es el tiempo total que tarda la

solicitud en viajar por la red más el tiempo de la respuesta que hace el viaje inverso. Por lo general, puede medir el RTT en milisegundos. Un RTT más bajo mejora la experiencia de uso de una aplicación y hace que esta responda mejor.

DNS (Sistema de Nombres de Dominio). El sistema de nombres de dominio (DNS) convierte los nombres de dominio en direcciones IP, que los navegadores utilizan para cargar páginas de Internet. Cada dispositivo conectado a Internet tiene su propia dirección IP, que es utilizada por otros dispositivos para localizar el dispositivo. Los servidores DNS permiten que las personas ingresen palabras normales en sus navegadores, como Fortinet.com, sin tener que hacer un seguimiento de la dirección IP de cada sitio web.

IaaS (Infraestructura como Servicio). IaaS, o infraestructura como servicio, es un modelo de cloud computing que ofrece acceso bajo demanda a recursos de computación, como servidores, almacenamiento, redes y virtualización.

IEC (Comisión Electrotécnica Internacional). La Comisión Electrotécnica Internacional (CEI), también conocida por su sigla en inglés IEC (International Electrotechnical Commission), es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.

IP (Protocolo de Internet). El Protocolo de Internet (IP) es un protocolo, o conjunto de reglas, para enrutar y direccionar paquetes de datos para que puedan viajar a través de las redes y llegar al destino correcto. Los datos que atraviesan Internet se dividen en trozos más pequeños, llamados paquetes.

IPv4 (Protocolo de Internet versión 4). IPv4 e IPv6 son dos versiones del sistema de direccionamiento del Protocolo de Internet (IP). La IP es un conjunto de reglas de comunicación que proporcionan el intercambio de datos a través de Internet. En esencia, Internet es una colección de miles de millones de dispositivos que comparten datos entre sí a través de tecnologías de red.

IPv6 (Protocolo de Internet versión 6). El Protocolo de Internet versión 6 (IPv6) es un conjunto de protocolos estándar para la capa de red de Internet.

ISO (Organización Internacional de Normalización). ISO es una organización internacional independiente y no gubernamental. Reúne a expertos de todo el mundo para acordar las mejores formas de hacer las cosas.

MAC (Control de Acceso al Medio). El Control de Acceso al Medio (MAC) se refiere a los métodos y protocolos utilizados para controlar el acceso a un medio de comunicación en una red informática. Es una subcapa de la Capa de Enlace de Datos en el modelo OSI y se encarga de la transmisión de paquetes de datos a través de un medio de red compartido.

MFA (Autenticación Multifactor). La autenticación multifactor (MFA) es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña.

NTC (Norma Técnica Colombiana). NORMÁS TECNICAS COLOMBIANAS (NTC). es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales.

NTP (Protocolo de Tiempo de Red). El Protocolo de Tiempo de Red (NTP) es un protocolo de internet que se utiliza para sincronizar las fuentes de tiempo del reloj de una computadora en una red. Pertenece y es uno de los componentes más antiguos del conjunto TCP/IP.

PCAP (Captura de Paquetes). La captura de paquetes, o PCAP, se refiere al proceso de interceptar y registrar paquetes de datos, que son las unidades de datos y carga útil que conforman el tráfico de red.

POST (Autoprueba de Encendido). Una autoprueba de encendido (POST) es una operación que inicia una computadora después de encenderla, pero antes de iniciar el sistema operativo.

QoS (Calidad de Servicio). La calidad de servicio (QoS) es el uso de mecanismos o tecnologías que funcionan en una red para controlar el tráfico y garantizar el rendimiento de aplicaciones críticas con capacidad de red limitada. Permite a las organizaciones ajustar su tráfico de red general al priorizar aplicaciones específicas de alto rendimiento.

SaaS (Software como Servicio). El software como servicio (SaaS) se considera tradicionalmente un modelo de software basado en la nube, el cual ofrece aplicaciones a los usuarios finales a través de un navegador de Internet. Los proveedores de SaaS alojan servicios y aplicaciones para que los clientes puedan acceder a ellos bajo demanda.

SFP+ (Pequeño Factor de Forma Conectable Plus). En el terreno rápidamente cambiante de la infraestructura de red, existe una demanda interminable de velocidades de transferencia de datos más rápidas y mejores formas de conectar dispositivos. Puertos Pluggable Plus (SFP+) de factor de forma pequeño Resultan útiles ya que proporcionan un método escalable y eficiente que se puede utilizar para lograr una transmisión de datos de alta velocidad.

SIEM (Gestión de Información y Eventos de Seguridad). es una solución de gestión de eventos e información de seguridad (SIEM). Estos tipos de soluciones recopilan, agregan y analizan grandes volúmenes de datos de aplicaciones, dispositivos, servidores y usuarios en toda la organización en tiempo real.

SLA (Acuerdo de Nivel de Servicio). Un acuerdo de nivel de servicio (SLA) es un contrato de proveedor de subcontratación y tecnología que define el nivel de servicio que dicho proveedor se compromete a brindar al cliente. Describe métricas como tiempo de actividad, tiempo de entrega, tiempo de respuesta y tiempo de resolución.

SOAR (Orquestación, Automatización y Respuesta de Seguridad). es una solución de software que permite a los equipos de seguridad integrar y coordinar herramientas de seguridad independientes, automatizar tareas repetitivas y agilizar los flujos de trabajo de respuesta a incidentes y amenazas.

SPAN (Analizador de Puerto Conmutado). El Analizador de Puertos de Conmutador (SPAN) es una herramienta específica del conmutador que copia las tramas Ethernet que pasan por los puertos del conmutador y las envía a un puerto específico.

TAP (Punto de Acceso al Tráfico). Un TAP de red es un dispositivo de hardware que se coloca en una red, especialmente entre dos de sus dispositivos conectados (como un switch, un router o un firewall) para monitorizar el tráfico de red.

TROUBLESHOOTING (Solución de problemas). Es la capacidad de diagnosticar y resolver un problema, una de las habilidades más difíciles de adquirir en un rol de TI no es el conocimiento técnico, sino la resolución efectiva de incidentes y problemas ya sea ayudando a los usuarios de forma presencial o remota.

APPLIANCE. Son dispositivos tecnológicos especializados que integran hardware y software en una sola solución, diseñados para cumplir funciones específicas dentro de una infraestructura de tecnología de la información, como el monitoreo, análisis y gestión del tráfico de red. Estos equipos se entregan preconfigurados o listos para su implementación, lo que permite una rápida puesta en funcionamiento, mayor eficiencia operativa y reducción de la complejidad en su administración.

2.2 APLICACIÓN

2.2.1 La presente especificación técnica aplica a la implementación de appliances para monitoreo y análisis avanzado de tráfico de red como sensores dentro de la infraestructura de comunicaciones del Ejército Nacional, integrados funcionalmente a la plataforma institucional de Network Detection and Response (NDR), su finalidad es ampliar la capacidad de visibilidad, análisis y detección en los dominios de red institucionales estos dispositivos se instalarán en las capas de núcleo (core), distribución y acceso de la infraestructura de red, así como en enlaces de interconexión críticos, el ámbito contempla tanto infraestructuras físicas (equipos y enlaces dedicados) como entornos virtualizados (switches virtuales, redes definidas por software y segmentos lógicos), incluyendo redes segmentadas y dominios de seguridad con distintos niveles de clasificación.

2.2.2 Los appliances deberán analizar el tráfico norte-sur (comunicaciones entre red interna y redes externas o perimetrales) y el tráfico este-oeste (comunicaciones internas entre servidores, usuarios, aplicaciones o segmentos de la misma red), permitiendo visibilidad integral del comportamiento de la infraestructura. La integración tecnológica con la solución NDR institucional y demás plataformas de monitoreo se realizará mediante interfaces estandarizadas y mecanismos seguros de intercambio de información, los dispositivos generarán telemetría estructurada, registros auditables y métricas operativas que soporten análisis comportamental, identificación de anomalías, detección de movimientos laterales y posibles exfiltraciones de información.

2.2.3 Durante las fases de instalación, integración y operación inicial se garantizará que el acceso a la infraestructura, configuraciones, topologías y registros de tráfico se realice bajo principios de mínimo privilegio, control de acceso y trazabilidad, los mecanismos de implementación preservarán la integridad, disponibilidad y confidencialidad de la información institucional tratada o generada por los appliances, evitando exposiciones no autorizadas o afectaciones a los activos críticos de la red.

2.2.4 Se debe cumplir con el ANEXO TÉCNICO DE ESPECIFICACIONES TÉCNICAS ADICIONALES, en caso de existir. Dicho anexo solo podrá establecer requisitos relacionados con perfiles profesionales, tiempos mínimos de experiencia, certificaciones del fabricante que respalden la calidad de los productos a entregar y actividades de transferencia de conocimiento, cuando así se requiera.

3 REQUISITOS

3.1 REQUISITOS GENERALES

No	ITEM	DESCRIPCION DE CARACTERISTICAS
3.1.1	EQUIPO	Los equipos appliances (Hardware) utilizados para el monitoreo y análisis de tráfico de red deberán ser entregados completamente instalados, configurados, integrados y puestos en funcionamiento de acuerdo con las necesidades operativas y de seguridad requeridas por el Ejército Nacional, los cuales deben ser originales de fábrica, nuevos y sin uso previo, con certificación

		de conformidad del fabricante, los cuales servirán para la seguridad de la infraestructura tecnológica del Ejército Nacional. Los equipos deberán ser plenamente compatibles e interoperables con la plataforma institucional de Network Detection and Response (NDR) actualmente desplegada, permitiendo integración directa sin requerir componentes adicionales que alteren la arquitectura existente. No se aceptarán soluciones que dependan de sensores virtuales externos, agentes complementarios no previstos o despliegues paralelos que puedan comprometer la seguridad, estabilidad o gobernanza del entorno tecnológico institucional.
3.1.2	SOPORTE FABRICANTE	Se deberá garantizar que los equipos adquiridos cuenten con soporte técnico oficial del fabricante, durante la vigencia requerida o la que sea establecida por el Ejército Nacional, bajo las siguientes condiciones mínimas: El servicio de soporte técnico deberá estar disponible bajo un esquema de atención 24x7x365, garantizando cobertura permanente durante las veinticuatro (24) horas del día, los siete (7) días de la semana y los trescientos sesenta y cinco (365) días del año, incluidos fines de semana y días festivos, sin interrupciones. Canales de atención: El acceso al soporte deberá realizarse a través de los canales oficiales del fabricante, incluyendo portal web especializado para gestión de casos, atención mediante correo electrónico corporativo y línea telefónica directa, conforme a los procedimientos y políticas establecidas por el fabricante para la administración de incidentes y solicitudes técnicas. Alcance del soporte: El alcance del soporte deberá cubrir la atención y resolución de incidentes asociados al hardware y software de los appliances suministrados, incluyendo fallas operativas, errores de funcionamiento, problemas de configuración, degradación del desempeño, vulnerabilidades identificadas y demás eventos técnicos que afecten la operación normal de la solución. Actualizaciones y parches: Derecho a recibir actualizaciones, parches de seguridad, correcciones y nuevas versiones liberadas por el fabricante durante la vigencia del contrato. En caso de presentarse fallas derivadas de una actualización, se deberá garantizar la reinstalación de la versión anterior sin generar costos adicionales para el Ejército Nacional.

		Tiempos de respuesta: El servicio de soporte técnico deberá regirse por los Acuerdos de Nivel de Servicio (SLA) definidos oficialmente por el fabricante, garantizando tiempos de respuesta y resolución acordes con la clasificación de severidad y criticidad del incidente reportado. La atención de eventos deberá contemplar esquemas de priorización técnica, diferenciando incidentes críticos que afecten la disponibilidad o integridad del servicio, incidentes de impacto medio relacionados con degradación funcional y eventos de baja criticidad asociados a consultas técnicas o ajustes de configuración. El proveedor deberá asegurar el cumplimiento de los tiempos máximos de respuesta inicial, escalamiento y resolución establecidos en los SLA del fabricante, incluyendo, cuando aplique, soporte remoto especializado y mecanismos de reemplazo de hardware bajo esquemas de garantía avanzada, con el fin de preservar la continuidad operativa de la solución. Escalamiento: El servicio de soporte técnico deberá permitir el escalamiento a niveles especializados del fabricante cuando la criticidad o complejidad del incidente lo requiera, garantizando atención oportuna por personal certificado y cumplimiento de los Acuerdos de Nivel de Servicio (SLA). La cobertura deberá prestarse sin costos adicionales, durante toda la vigencia contractual y en idioma español, asegurando continuidad operativa y trazabilidad de los casos. En caso de falla del equipo, el fabricante deberá efectuar el reemplazo por uno de iguales o superiores características técnicas, plenamente compatible con la infraestructura existente, conforme a los tiempos definidos en los SLA, incluyendo asistencia remota especializada. El contratista será responsable de coordinar la gestión y seguimiento de los casos con el fabricante, en articulación con el personal técnico designado por el Ejército Nacional.
3.1.3	SOPORTE CONTRATISTA	El contratista deberá garantizar la prestación de un servicio de soporte técnico bajo un esquema de disponibilidad 24x7, es decir, veinticuatro (24) horas al día, siete (7) días a la semana, a partir del inicio de ejecución y durante toda la vigencia contractual. El soporte deberá prestarse en modalidad remota y, cuando la naturaleza del incidente lo requiera o la Entidad lo determine, en modalidad presencial, asegurando continuidad operativa y tiempos de atención acordes con la criticidad del evento.

		El servicio deberá contemplar recepción, registro, clasificación, diagnóstico, escalamiento y cierre de incidentes, garantizando trazabilidad y seguimiento técnico hasta su solución definitiva. Canales de atención: Los canales de atención deberán incluir, como mínimo, acceso mediante portal web para gestión de casos, atención a través de correo electrónico corporativo y línea telefónica directa, conforme al esquema oficial de soporte definido, asegurando disponibilidad permanente y mecanismos formales de registro y control de solicitudes. Alcance del soporte: El servicio de soporte deberá cubrir la atención integral de incidentes técnicos asociados a los appliances suministrados, incluyendo fallas de hardware, errores de funcionamiento del software, degradación del desempeño, indisponibilidad parcial o total del servicio y anomalías detectadas durante su operación. Asimismo, deberá contemplar la gestión de problemas de configuración, ajustes de parametrización, incompatibilidades de integración con la plataforma y demás componentes de la infraestructura tecnológica institucional, así como la identificación, análisis y mitigación de vulnerabilidades que puedan afectar la seguridad, estabilidad o interoperabilidad de la solución. La atención deberá abarcar el diagnóstico, corrección, aplicación de actualizaciones de firmware o parches de seguridad, validación posterior a la intervención y restablecimiento del servicio en condiciones óptimas de operación, garantizando la adecuada integración y funcionamiento continuo dentro de la arquitectura tecnológica del Ejército Nacional. Tiempos de respuesta: El servicio de soporte técnico deberá garantizar atención prioritaria y oportuna frente a cualquier incidente que afecte la operación de los appliances. Para eventos clasificados como críticos, el tiempo máximo de respuesta inicial no deberá superar las cuatro (4) horas contadas a partir del registro formal del caso por los canales oficiales definidos. Dicha respuesta deberá incluir confirmación de recepción, categorización de severidad, diagnóstico preliminar y definición de acciones técnicas orientadas a la contención y restablecimiento del servicio. La atención podrá realizarse en modalidad remota o presencial, según la naturaleza del evento y su impacto en la infraestructura tecnológica, asegurando en todo momento la continuidad operativa y la integridad de los servicios soportados. Cualquier costo derivado de fallas, daños, defectos de funcionamiento, reposición de componentes, reemplazo de

		equipos, desplazamientos, mano de obra especializada, configuraciones, pruebas técnicas o actividades necesarias para la recuperación y restablecimiento del servicio deberá ser asumido en su totalidad por el proveedor, sin que ello represente erogación adicional alguna para el Ejército Nacional. El servicio de soporte técnico, instalación, mantenimiento y demás actividades asociadas a la operación de los appliances deberá prestarse con cobertura en cualquier ciudad o municipio del territorio Nacional donde el Ejército Nacional disponga infraestructura tecnológica o determine su despliegue. El proveedor deberá garantizar capacidad operativa y disponibilidad de recurso técnico idóneo para atender requerimientos en cualquier punto del país, considerando que la infraestructura institucional tiene alcance Nacional. La prestación del servicio deberá efectuarse sin limitaciones geográficas, asegurando continuidad operativa, tiempos de atención acordes con la criticidad del incidente y condiciones técnicas homogéneas en todos los lugares de operación.
3.1.4	DOCUMENTACIÓN	Como parte integral de la implementación y puesta en operación de los appliances, deberá entregarse la documentación técnica completa, actualizada y en idioma español, en formato digital editable (según corresponda: PDF, Word, Excel, Visio u otros formatos técnicos estándar). La información suministrada deberá permitir la administración, operación, mantenimiento y sostenibilidad técnica de la solución dentro de la infraestructura institucional. La documentación técnica deberá incluir, como mínimo: Manuales detallados de instalación, configuración, operación, administración y mantenimiento preventivo y correctivo del appliance, alineados con las mejores prácticas del fabricante. Diagramas de arquitectura de despliegue y topología de red implementada, en formatos gráficos y editables, que reflejen claramente los puntos de interconexión, segmentación y ubicación lógica y física del equipo. Procedimientos Operativos Estándar (SOP) para actividades rutinarias y críticas, incluyendo gestión de eventos, actualizaciones, respaldos, restauración y validación operativa. Matriz técnica de integración con los sistemas existentes, especificando interfaces, protocolos, puertos, dependencias técnicas y mecanismos de interoperabilidad utilizados. Guía estructurada de resolución de problemas (troubleshooting), que incorpore metodologías de diagnóstico, árboles de decisión y

		lineamientos para identificación y solución de fallas, así como directrices técnicas para configuración y validación de integraciones mediante APIs cuando aplique. Documento de cierre técnico de implementación que contenga inventario detallado de equipos (modelo, número de serie), versiones de firmware y software instaladas, resultados de pruebas funcionales y de desempeño, métricas iniciales de operación, evidencias técnicas y análisis de riesgos técnicos residuales con recomendaciones de optimización o escalabilidad futura. La documentación deberá mantenerse actualizada frente a cualquier ajuste técnico, modificación de configuración o mejora implementada en la solución, garantizando que la información refleje en todo momento el estado real de la arquitectura desplegada y su operación dentro de la infraestructura tecnológica institucional.
3.1.5	NORMATIVIDAD APLICABLE	Los bienes y servicios TIC asociados a la presente especificación técnica deberán garantizar soporte nativo para el Protocolo de Internet versión seis (IPv6), en coexistencia con IPv4 (doble pila – dual stack), en cumplimiento de lo establecido en la Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) mediante la Resolución 2710 de 2017, particularmente lo dispuesto en su artículo 5°, el cual exige que en los procesos de contratación de bienes y servicios relacionados con TIC se incluya soporte IPv6 nativo.
3.1.6	GARANTÍA	GARANTÍA TÉCNICA Y TIEMPOS DE RESPUESTA El servicio de soporte técnico deberá prestarse durante el período de garantía definido para los equipos, conforme a las condiciones ofrecidas por el fabricante y a los requerimientos técnicos establecidos por el Ejército Nacional en la presente especificación. Durante dicho período, deberán atenderse de manera prioritaria y oportuna los requerimientos técnicos reportados por el personal designado, asegurando diagnóstico, gestión y solución de incidentes asociados al funcionamiento del hardware y software de los appliances. La prestación del soporte deberá ejecutarse en estricta observancia de las condiciones técnicas de garantía del fabricante y de los lineamientos definidos en la presente especificación, garantizando continuidad operativa, integridad de la solución y cumplimiento de los estándares de calidad aplicables a bienes y servicios TIC en el sector público. NIVELES DE SERVICIO (SLA) Se deberá garantizar los siguientes tiempos de atención diferenciados según criticidad del incidente, impacto operativo, nivel de riesgo para la seguridad de la información, ubicación geográfica del equipo, necesidad de intervención remota o presencial y disponibilidad de repuestos o reemplazo.

		Tiempo máximo de respuesta inicial: hasta cuatro (4) horas, contadas a partir del reporte formal del incidente por parte del Ejército Nacional. Atención remota o presencial: Cuando la naturaleza, complejidad o impacto del incidente requiera intervención, deberá disponerse de personal técnico especializado. La modalidad de atención (remota o presencial) se determinará según la criticidad del evento y las capacidades de diagnóstico remoto disponibles. Los tiempos de desplazamiento y atención presencial deberán definirse en función de la criticidad del incidente, el nivel de afectación del servicio y la ubicación geográfica donde deba efectuarse la intervención. Considerando la distribución geográfica de los appliances en distintos puntos del territorio nacional, dichos tiempos serán establecidos por el Ejército Nacional conforme a sus prioridades operativas y deberán ser cumplidos por el proveedor. Tiempo máximo de restablecimiento del servicio: Para incidentes críticos que afecten la operación de ciberdefensa y monitoreo de red institucional, los tiempos de restablecimiento se establecen de manera diferenciada según el tipo de solución requerida: Solución remota (configuración, actualización, reinicio o diagnóstico sin reemplazo físico): hasta cuatro (4) horas posteriores al reporte formal del incidente. Solución presencial con reemplazo físico de componentes o desplazamiento a zonas distantes: hasta ocho (8) horas posteriores al reporte formal del incidente, siempre que las condiciones técnicas, geográficas y de disponibilidad de repuestos lo permitan, en el evento que se requiera un tiempo mayor para el remplazo físico el contratista deberá indicar las circunstancias de fuerza mayor que impliquen un tiempo mayor que el otorgado inicialmente, todo esto conforme a criterios de razonabilidad, proporcionalidad y debida diligencia contractual. El tiempo de respuesta se contabilizará desde la notificación oficial y estará condicionado a: • Condiciones técnicas del equipo o sistema. • Ubicación geográfica del lugar de instalación. • Restricciones logísticas, de movilidad o de seguridad. • Disponibilidad efectiva e inmediata de repuestos originales o compatibles certificados.

		• Condiciones de orden público o factores externos que incidan en el desplazamiento. Cuando circunstancias externas, imprevisibles e irresistibles impidan el cumplimiento del tiempo inicialmente previsto, deberá informarse de manera inmediata la situación presentada, exponiendo técnicamente las causas y aportando los soportes correspondientes. En tal evento, se deberá indicar el nuevo tiempo estimado de solución y las medidas de mitigación implementadas para garantizar la continuidad operativa del servicio. En caso de que el restablecimiento del servicio requiera actividades adicionales por parte del fabricante, sustitución de componentes no disponibles localmente o condiciones geográficas especiales debidamente justificadas, el contratista deberá informar oportunamente al Ejército Nacional y ejecutar las acciones necesarias para la mitigación del impacto operativo, garantizando siempre una respuesta proporcional al nivel de riesgo y afectación del servicio. Durante el período establecido se responderá por la atención de fallas, defectos de fabricación, degradación del servicio y cualquier otra situación cubierta por la garantía técnica, sin que ello genere costos adicionales para el Ejército Nacional. Durante la vigencia de la garantía técnica, cualquier falla, daño o defecto de funcionamiento de los appliances será atendido conforme a los niveles de servicio aquí establecidos. Durante el periodo establecido se responderá por la atención de fallas, defectos de fabricación, degradación del servicio y cualquier otra situación cubierta por la garantía técnica, sin que ello genere costos adicionales para la Entidad. Durante la vigencia de la garantía técnica, cualquier falla, daño, defecto de funcionamiento o degradación que se presente en los appliances, independientemente de su ubicación dentro del territorio nacional, deberá ser atendida íntegramente por el Contratista. En caso de requerirse el reemplazo total o parcial de un appliance, o el cambio de cualquiera de sus componentes, partes o accesorios, en cualquier ciudad, municipio o unidad del territorio nacional de Colombia, el Contratista deberá asumir la totalidad de los costos asociados, incluidos, sin limitarse a: • Transporte y logística a nivel nacional • Desplazamiento del personal técnico especializado • Retiro, instalación y reinstalación de equipos • Configuración, puesta en funcionamiento y pruebas

		• Coordinación con el fabricante y trámites de garantía Lo anterior se realizará sin generar ningún costo adicional para la Entidad, y sin que la ubicación geográfica del appliance sea considerada causal de limitación, excepción o cobro adicional dentro de la ejecución del contrato.
3.1.7	PROCESO DE INSTALACIÓN Y PUESTA EN OPERACIÓN	La instalación e integración de la solución contemplará el montaje físico del appliance en un rack estándar de 19 pulgadas, su conexión a la UPS institucional y el etiquetado conforme a los lineamientos definidos por la Entidad. Posteriormente, se realizará la configuración básica del equipo, incluyendo la definición de direcciones IP de gestión, parámetros de DNS, NTP y rutas necesarias para su correcta operación. A continuación, se deberá incluir la configuración y habilitación de los puertos necesarios para la adquisición del tráfico de red, mediante el uso de mecanismos estándar como SPAN, TAP u otros técnicamente equivalentes, garantizando que la captura del tráfico se realice sin afectar el desempeño de la red productiva y manteniendo un nivel de integridad y confiabilidad acorde con las capacidades y buenas prácticas definidas por el fabricante. Seguidamente, durante la configuración, instalación y puesta en funcionalidad, se deberá realizar la asociación del sensor con el componente central (Master), asegurando su correcto registro dentro de la plataforma de administración. Este proceso incluirá la validación del enlace de comunicación, la verificación de que el sensor sea reconocido, gestionado y monitoreado desde la Master, y la confirmación de su operación adecuada, garantizando que el intercambio de información se realice de manera estable, segura y conforme a las capacidades del fabricante. Se deberá validar y supervisar la recepción y el procesamiento de los datos durante un período inicial de observación no inferior a ocho (8) horas, con el objetivo de confirmar la estabilidad, continuidad y correcto funcionamiento, asegurando que la información sea recibida y procesada de manera consistente y sin interrupciones. Se deberán aplicar los ajustes finales que sean necesarios, incluyendo la definición de excepciones operativas y un proceso de afinamiento inicial (tuning), orientados a optimizar el desempeño del sistema y reducir el ruido operativo, de acuerdo con las necesidades del Ejército Nacional.
3.1.8	LEVANTAMIENTO DE INFORMACIÓN	El deberá llevar a cabo un levantamiento técnico exhaustivo antes de la implementación, con el objetivo de identificar y documentar las fuentes de tráfico de red que serán monitoreadas. Esto incluirá la identificación de los puntos de captura mediante puertos SPAN (Switched Port Analyzer) o dispositivos TAP (Terminal Access

		Point), el esquema de direccionamiento IP para los appliances de gestión y análisis, así como la arquitectura de red existente en las ubicaciones donde se desplegarán los equipos. A partir de este levantamiento, se deberá presentar para la aprobación del Ejército Nacional un diseño técnico detallado que incluya diagramas de topología, una matriz de fuentes de tráfico, un plan de direccionamiento, requisitos de ancho de banda, especificaciones de conectividad y puntos de integración con la infraestructura actual.

3.2 REQUISITOS ESPECÍFICOS

3.2.1 APPLIANCE (HARDWARE)		
No	**ITEM**	**DESCRIPCIÓN DE CARACTERÍSTICAS**
3.2.1.1	Factor de forma	Appliance para montaje en rack estándar, con factor de forma máximo 1U, apto para la instalación en centros de datos institucionales.
3.2.1.2	Compatibilidad de rack	El equipo deberá ser compatible con rack estándar de 19 pulgadas.
3.2.1.3	Dimensiones	El equipo deberá tener compatibilidad con equipos de hasta **1U**, con profundidad **máxima aproximada de 45 cm**, que permita su instalación en racks existentes sin requerir adecuaciones especiales.
3.2.1.4	Peso	Peso máximo aproximado de 7 kg, incluyendo componentes internos, que facilite su instalación y mantenimiento en sitio.
3.2.1.5	Fuente de alimentación	El equipo debe contar con mínimo 01 fuente de alimentación interna, con alimentación eléctrica 100–240 V CA, autorango, conector estándar tipo IEC o equivalente, cumpliendo normas internacionales de seguridad eléctrica.
3.2.1.6	Consumo eléctrico	El equipo deberá contar con las siguientes características de consumo eléctrico, así: • estado inactivo: Consumo eléctrico en estado inactivo máximo de 30 W.

		• carga típica: Consumo eléctrico a carga típica de operación (aproximadamente 80–85 %) máximo de 100 W. Igualmente, deberá tener un máximo de Consumo eléctrico que no supere a los 120 W.
3.2.1.7	Interfaz de administración	El equipo deberá contar con una interfaz de red dedicada para administración, tipo 10/100/1000 BASE-T o superior.
3.2.1.8	Interfaz de gestión remota	El equipo deberá contar con una interfaz de red dedicada para la gestión remota, tipo 10/100/1000 BASE-T o superior, la cual podrá ser dedicada o compartida según el diseño del fabricante.
3.2.1.9	Interfaces de análisis (cobre)	Mínimo tres (3) interfaces de red para análisis de tráfico, tipo 10/100/1000 BASE-T o superior, dedicadas o configurables según el diseño del fabricante.
3.2.1.10	Capacidad de expansión	El appliance deberá soportar al menos un (1) módulo de expansión activo simultáneamente, o una arquitectura equivalente que permita la ampliación de interfaces de red.
3.2.1.11	Módulos de expansión	El equipo deberá soportar y permitir la instalación de módulos de expansión o soluciones funcionalmente equivalentes, y deberá incluir como mínimo uno (1) de los siguientes módulos, conforme a las necesidades del Ejército Nacional • Módulo de expansión – Cobre (1G): Soporte para módulos de expansión o soluciones equivalentes que incluyan dos (2) puertos RJ45 1000BASE-T. • Módulo de expansión – Cobre (1G) de mayor capacidad: Soporte para módulos de expansión o soluciones funcionalmente equivalentes que incluyan hasta cuatro (4) puertos RJ45 1000BASE-T, o una arquitectura equivalente que permita dicha capacidad.

3.2.2 CAPACIDADES MÍNIMAS DE PROCESAMIENTO (THROUGHPUT / CONEXIONES / ACTIVOS)		
No	**ITEM**	**DESCRIPCIÓN DE CARACTERÍSTICAS**
3.2.2.1	Perfil de capacidad – Tipo 1 (Principal)	Capacidad mínima 250.000 conexiones por minuto, throughput efectivo mínimo de 5 Gbps y capacidad de análisis de hasta 50.000 dispositivos, o capacidades funcionalmente equivalentes o superiores.
3.2.2.2	Perfil de capacidad – Tipo 2 (Pro)	Capacidad mínima 50.000 conexiones por minuto, throughput efectivo mínimo de 2 Gbps y capacidad de análisis de hasta 8.000 dispositivos, o capacidades funcionalmente equivalentes o superiores.
3.2.2.3	Procesamiento pasivo (fuera de línea)	El appliance deberá operar bajo un esquema de procesamiento pasivo (fuera de línea), recibiendo el tráfico mediante puertos pasivos tipo SPAN, TAP o mecanismos técnicamente equivalentes, sin introducir retardos, pérdida de paquetes ni impacto en el desempeño de la red productiva.

3.2.3 SOFTWARE REQUISITOS FUNCIONALES		
No	**ITEM**	**DESCRIPCIÓN DE CARACTERÍSTICAS**
3.2.3.1	Software embebido y preinstalado	El appliance deberá contar con las funcionalidades de análisis y seguridad preinstaladas e integradas de fábrica, como parte esencial e inseparable del equipo.
3.2.3.2	Prohibición de componentes externos	El sistema no debe tener componentes que deban instalarse en servidores de propósito general.
3.2.3.3	Prohibición de vSensor u otros despliegues	No se aceptarán arquitecturas que dependan obligatoriamente de despliegues adicionales tipo vSensor u otros componentes externos para su funcionamiento base.
3.2.3.4	Operación como sensor de red	Debe operar como sensor recibiendo tráfico desde uno o varios switches mediante mecanismos estándar (p. ej., SPAN/TAP).

3.2.3.5	Detección en tiempo real	Deberá permitir la detección y gestión de comportamientos anómalos en tiempo cercano a tiempo real, mediante analítica avanzada e IA/ML o enfoques equivalentes.
3.2.3.6	IA y Machine Learning	La solución deberá emplear múltiples modelos analíticos, incluyendo técnicas de inteligencia artificial y aprendizaje automático, para identificar desviaciones de comportamiento.
3.2.3.7	Autoaprendizaje y enfoque adaptativo	Debe ser una plataforma de autoaprendizaje con línea base adaptable/dinámica ante cambios del entorno.
3.2.3.8	Prohibición de reglas/firmas como base	La detección de amenazas deberá basarse principalmente en el análisis de comportamiento, no en tecnologías de reglas o firmas estáticas como fundamento principal.
3.2.3.9	No firmas/reglas/heurística/sandboxing	La identificación de amenazas no deberá depender exclusivamente de firmas, reglas, heurística tradicional o sandboxing.
3.2.3.10	Alertamiento automático	Debe alertar automáticamente sobre todas las actividades inusuales y anormales en la red.
3.2.3.11	Auditoría de dispositivos	Debe proporcionar seguimiento/auditoría de dispositivos, mostrando al menos: tipo, hostname, MAC, primera y última vez visto.
3.2.3.12	Análisis de comportamiento (mínimos)	Debe resaltar al menos: conectividad inusual; actividades inusuales; historial IP (incl. DHCP); seguimiento de usuario/credencial y hostnames asociados; volúmenes de conexiones inusuales; rareza de dispositivo y rareza de acceso a sitio externo.
3.2.3.13	Detección de comportamiento anómalo	Debe identificar comportamientos anómalos y resaltarlos en tiempo real.
3.2.3.14	Descubrimiento de dispositivos nuevos	Debe identificar cualquier dispositivo nuevo insertado en la red.
3.2.3.15	Captura de paquetes	Debe permitir captura de paquetes en tiempo real para análisis del incidente; con opción de analizar en Wireshark y/o dentro de su propia interfaz.
3.2.3.16	Personalización del ML	Debe permitir personalización/adaptación del aprendizaje automático a condiciones específicas de la red.

3.2.3.17	Integración con LDAP	Debe tener integración con LDAP.
3.2.3.18	Parámetros avanzados de verificación	Debe permitir personalización avanzada considerando múltiples parámetros, incluyendo al menos: conexiones (externas/internas), transferencia de datos (externa), conexiones SMB internas, conexiones a puerto cerrado, difusiones, dispositivos conectados, transferencia de datos (cliente/servidor).
3.2.3.19	Modelado por usuario/dispositivo/red	Debe modelar comportamiento normal a nivel de usuario, dispositivos y red, e identificar autónomamente anomalías asociadas a brechas.
3.2.3.20	Aprendizaje sin historial previo	Debe aprender el comportamiento normal sin requerir historial de comportamiento anómalo, con posibilidad de identificar amenazas desde el primer día.
3.2.3.21	Amenazas internas y externas	Debe detectar amenazas internas y externas.
3.2.3.22	Tipos mínimos de brechas	Debe detectar como mínimo: botnet, gusanos, ransomware, infiltración/exfiltración, credenciales comprometidas, minería de bitcoins, malware, DDoS vía IoT, APT.
3.2.3.23	Operación en sitio (on-prem)	La solución deberá operar en sitio (on-premises), sin requerir obligatoriamente servicios en la nube para el análisis principal.
3.2.3.24	Detección de amenazas nuevas	Debe reconocer nuevas amenazas no advertidas previamente.
3.2.3.25	Exclusión tecnológica	No se aceptarán soluciones tipo firewall, NGFW, SIEM o sandboxing como sustituto funcional de la solución solicitada.
3.2.3.26	Interfaz de visualización	Debe poseer una interfaz de visualización intuitiva.
3.2.3.27	Visualización con profundidad	Deberá ofrecer visibilidad profunda a nivel de dispositivos y conexiones en tiempo real, sin requerir compartir información con nubes globales para obtener inteligencia.
3.2.3.28	Tiempo real e histórico	Debe visualizar en tiempo real y permitir visualizar histórico de manera gráfica, con búsqueda por hora exacta.

3.2.3.29	Estado del sistema (panel)	Debe permitir consultar estado completo: versión de software, disco usado, consumo de CPU y memoria.
3.2.3.30	Estado de interfaces	Debe mostrar detalle de interfaces activas y tráfico recibido por cada una.
3.2.3.31	Métricas de ancho de banda	Debe mostrar: ancho de banda total actual, promedio a la fecha, últimos 7 días y 2 semanas anteriores.
3.2.3.32	Visibilidad de protocolos	Debe mostrar análisis del tráfico y última vez vistos protocolos principales, incluyendo: HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos.
3.2.3.33	Visibilidad de datos de red	Debe dar visibilidad en tiempo real de: cantidad de servidores, cantidad de estaciones cliente, cantidad de credenciales de usuario y tráfico de red.
3.2.3.34	Búsqueda rápida	Debe permitir encontrar elementos por: IP/tipo de dispositivo, función/protocolo conocido (DNS/AD), nombre del dispositivo.
3.2.3.35	Detalle de dispositivo	Al buscar un dispositivo debe mostrar como mínimo: IP, MAC, sistema operativo, logs de eventos, logs de brechas identificadas, historial de conexiones, lista de dispositivos similares.
3.2.3.36	Visibilidad de amenazas (logs)	Debe mostrar amenazas identificadas en tiempo real con el detalle de logs de cada amenaza.
3.2.3.37	Amenaza en gráfico	Debe mostrar la amenaza de manera gráfica y en tiempo real.
3.2.3.38	Criticidad	Debe agrupar anomalías por nivel de criticidad.
3.2.3.39	Gestión centralizada	La solución debe ser centralizada: administración y visualización para gobernar y monitorear el entorno.
3.2.3.40	Análisis centralizado (datacenter principal)	El análisis con IA/Machine Learning debe realizarse de manera centralizada del tráfico proveniente del datacenter principal (según arquitectura de la Entidad).
3.2.3.41	Modos de implementación	Debe soportar al menos: Port mirror (SPAN) y TAP (externo).
3.2.3.42	Backup/Restore	Debe permitir backup y restore de la configuración, incluyendo programación de backups.

3.2.3.43	Respuesta autónoma	Debe generar respuestas autónomas cuando surge un incidente anómalo, interrumpiendo actividad maliciosa manteniendo operaciones normales.
3.2.3.44	Modo pasivo/activo	Debe poder configurarse en modo pasivo o activo según configuración del administrador.
3.2.3.45	Ventana de contención	Debe detener la anomalía/amenaza hasta en un plazo de 24 horas recurrentes mientras el equipo de ciberseguridad toma acciones correctivas.

3.2.4 IMPLEMENTACIÓN	
3.2.4.1	Se deberá ejecutar un plan de validación e implementación con el fin de verificar el correcto funcionamiento, la adecuada instalación y la puesta en operación de los appliances, el cual será revisado y validado por el Supervisor del contrato y el personal técnico designado. Dicho plan contemplará la definición clara de actividades, responsables, y será desarrollado mediante la elaboración de un plan técnico de instalación detallado, el cual incluirá los siguientes términos: • Levantamiento de Infraestructura: Un análisis previo de la infraestructura de red existente. • Identificación de Fuentes de Tráfico de red: Determinación de las fuentes de tráfico críticas que se deberán monitorear. • Definición de Puntos de Captura: Especificación de los puntos de captura mediante puertos SPAN o dispositivos TAP. • Esquema de Direccionamiento IP: Planificación del direccionamiento IP para los appliances. • Requisitos de Conectividad y Ancho de Banda: Definición de los requisitos necesarios para asegurar un funcionamiento óptimo. • Diagramas de Topología: Presentación de diagramas de topología física y lógica propuestos. • Matriz de Integración: Creación de una matriz que conecte con los sistemas actuales, como SIEM, consolas de gestión y el sistema Master existente. • Cronograma de Actividades: Un cronograma que incluya hitos y entregables. • Ventanas de Mantenimiento: Identificación de las ventanas de mantenimiento para minimizar el impacto operativo. • Recursos Técnicos y Humanos: Detalle de los recursos necesarios para la implementación. • Análisis de Riesgos: Evaluación de riesgos potenciales y desarrollo de planes de contingencia. Este diseño será presentado formalmente al Ejército Nacional para su revisión,

	ajustes y validación conjunta por parte del equipo técnico designado. Este proceso garantizará que la propuesta de implementación se encuentre alineada con las necesidades operativas, las restricciones de seguridad, las políticas institucionales y la arquitectura de red de la Fuerza. El plan deberá contar con la aprobación formal mediante acta firmada por el Supervisor del contrato, como requisito previo a la ejecución de cualquier actividad de implementación en el entorno productivo.
3.2.4.2	**IMPLEMENTACIÓN FÍSICA Y LÓGICA** Esta fase abarca la ejecución del plan de instalación aprobado, comenzando con la implementación física, que incluye: • Montaje de Appliances: Instalación de los appliances en los racks designados. • Conexión a Sistemas de Alimentación: Conexión a sistemas de alimentación eléctrica regulada y respaldada por UPS. • Cableado Estructurado: Realización del cableado estructurado para las interfaces de red, tanto para gestión como para captura de tráfico. • Verificación de Condiciones Ambientales: Comprobación de que las condiciones ambientales sean adecuadas, incluyendo temperatura, humedad y ventilación. • Etiquetado e Inventario: Etiquetado e inventario de los equipos, registrando números de serie y ubicaciones. La implementación lógica comprende: • Configuración Inicial de Appliances: Configuración inicial de los appliances, incluyendo parámetros de red como direccionamiento IP, gateway y máscaras de subred. • Servicios Básicos: Configuración de servicios básicos como DNS y NTP para la sincronización de tiempo. • Asociación con el Master: Asociación y registro con el componente central de gestión existente en la infraestructura institucional. • Configuración de Puertos de Captura: Configuración de puertos de captura en modo promiscuo para la ingestión de tráfico. • Políticas de Segmentación de Red: Establecimiento de políticas de segmentación de red mediante VLANs. • Controles de Acceso: Implementación de controles de acceso a las consolas de administración. • Habilitación de Módulos: Activación de módulos y funcionalidades licenciadas, como módulos de analítica avanzada, respuesta automática y funcionalidades de seguridad licenciadas. • Configuración de Parámetros Iniciales: Configuración de los parámetros iniciales de retención de datos, alertas y umbrales básicos. Todo el proceso será documentado mediante bitácoras técnicas, capturas de pantalla de las configuraciones aplicadas y evidencias fotográficas de la instalación física.

	PRUEBAS Y AJUSTES (OPTIMIZACIÓN DE INGESTIÓN, LATENCIA INTERNA) Se deberá llevar a cabo un protocolo exhaustivo de pruebas técnicas para validar el correcto funcionamiento de los appliances. Este proceso comenzará con pruebas de ingestión de tráfico, cuyo objetivo es verificar que los appliances están capturando efectivamente los flujos de red desde las fuentes configuradas. Se medirán las tasas de captura, se identificarán posibles pérdidas de paquetes y se validará que el throughput procesado corresponda al volumen esperado según el dimensionamiento realizado. Se realizarán ajustes de optimización de la ingestión mediante la configuración de buffers, el ajuste de políticas de muestreo cuando sea necesario, y la optimización de los recursos de procesamiento para garantizar una captura completa sin degradación del rendimiento.
3.2.4.3	Las pruebas de latencia interna evaluarán los tiempos de procesamiento desde la captura del paquete hasta su análisis por los motores analíticos y capacidades avanzadas del sistema, la generación de alertas y la disponibilidad en las interfaces de consulta. Se realizarán ajustes en la arquitectura de procesamiento, en la distribución de carga entre appliances y en la optimización de consultas para asegurar tiempos de respuesta adecuados. Además, se ejecutarán pruebas de correlación de eventos mediante la simulación de patrones anómalos conocidos (como escaneos, exfiltraciones y movimientos laterales) para validar la capacidad de detección. También se llevarán a cabo pruebas de integración con sistemas externos (exportación de alertas a SIEM y APIs de consulta), pruebas de resiliencia mediante reinicios controlados, y pruebas de rendimiento bajo condiciones de carga normal y picos de tráfico. Todos los resultados serán documentados con métricas cuantitativas, gráficas de rendimiento y evidencias técnicas.
3.2.4.4	**ACOMPAÑAMIENTO Y RECOMENDACIÓN DE TUNING** Durante el período de puesta en funcionamiento y en caso de presentarse problemas posterior a la entrega se deberá realizar el respectivo acompañamiento técnico, cuya duración será definida y autorizada por el Supervisor del contrato, se deberá proporcionar acompañamiento técnico continuo, con el propósito de supervisar el proceso de estabilización y el aprendizaje de las capacidades analíticas y de detección del sistema, permitiendo la correcta identificación de los patrones normales de comportamiento de la red institucional y asegurando una operación adecuada conforme a los lineamientos establecidos. Este acompañamiento incluirá revisiones periódicas de las alertas generadas (diarias durante la primera semana y posteriormente con una periodicidad semanal), con el objetivo de identificar y reducir la ocurrencia de falsos positivos. Adicionalmente, se realizará el análisis de los dispositivos y servicios descubiertos

	en la red para validar la completitud del inventario automático, así como la evaluación de la evolución de los modelos o mecanismos de análisis mediante métricas objetivas de desempeño, precisión o indicadores equivalentes funcionalmente comparables. En el marco de este proceso, se identificarán posibles zonas de la red con visibilidad insuficiente que requieran ajustes en los puntos de captura, así como eventuales problemas de rendimiento o configuración. Con base en los resultados obtenidos, deberá elaborar recomendaciones técnicas de ajuste fino (tuning), sin afectar la cobertura de monitoreo requerida ni las capacidades mínimas de detección definidas contractualmente, las cuales podrán incluir, entre otras: • Configuración de listas de exclusión o mecanismos equivalentes para servicios legítimos que generen alertas recurrentes. • Ajuste de umbrales de sensibilidad o parámetros equivalentes para determinados tipos de eventos o amenazas, de acuerdo con el contexto operacional. • Configuración de políticas de agrupación o correlación de alertas para la reducción de ruido operativo. • Optimización de reglas o mecanismos de correlación de eventos. • Recomendaciones de segmentación adicional de la red con el fin de mejorar la granularidad del análisis. • Recomendaciones no vinculantes de escalamiento de recursos, en caso de identificarse limitaciones de capacidad frente a los perfiles contratados. Las recomendaciones serán presentadas de manera formal, incluyendo su justificación técnica, el impacto esperado y una priorización para su implementación progresiva, quedando su aplicación sujeta a la aprobación del supervisor del contrato.
3.2.4.5	**ENTREGA DE INFORME CONSOLIDADO Y DOCUMENTACIÓN FINAL** Al finalizar el proyecto de implementación, deberá entregar un **informe consolidado integral**, en el cual se documente de manera completa y trazable todo el ciclo de vida del proyecto. Dicho informe deberá incluir, como mínimo, los siguientes componentes: • **Resumen Ejecutivo:** Síntesis de los objetivos alcanzados, principales actividades ejecutadas, desafíos presentados y estado final de la implementación. • **Inventario Completo:** Inventario de los equipos instalados, incluyendo como mínimo números de serie, ubicaciones físicas, direcciones IP asignadas y versiones de software y firmware. • **Diagramas Actualizados:** Diagramas de topología física y lógica de la red, que reflejen la ubicación de los appliances, los puntos de captura configurados, los flujos de tráfico monitoreados y la arquitectura de integración implementada. • **Detalle de Configuraciones:** Descripción de las configuraciones aplicadas,

	incluyendo parámetros de red, políticas de seguridad, parámetros o mecanismos de detección, integraciones con sistemas externos y personalizaciones realizadas. • **Resultados de Pruebas:** Resultados completos de las pruebas ejecutadas, incluyendo métricas de desempeño tales como throughput, latencia y tasas de captura, así como evidencias técnicas (capturas de pantalla, registros de eventos, gráficas) y la validación de los criterios de aceptación. • **Estadísticas del Período de Puesta en Funcionamiento:** Estadísticas del periodo de estabilización, que incluyan dispositivos descubiertos, servicios identificados, volumen de tráfico procesado, alertas generadas por categoría, incidentes analizados y la evolución de los mecanismos de análisis y detección basados en comportamiento o capacidades funcionalmente equivalentes. • **Recomendaciones de Tuning:** Relación de los ajustes realizados y pendientes, incluyendo su justificación técnica y nivel de prioridad. • **Matriz de Riesgos Residuales:** Identificación de riesgos residuales, con su probabilidad, impacto y controles de mitigación sugeridos. • **Recomendaciones de Escalamiento Futuro:** Recomendaciones técnicas no vinculantes orientadas al crecimiento proyectado de la red o a la incorporación de nuevos casos de uso, sin generar obligación contractual ni compromiso presupuestal. • **Lecciones Aprendidas:** Buenas prácticas identificadas y oportunidades de mejora continua. La documentación final deberá incluir, como mínimo, manuales técnicos y de usuario actualizados conforme a la implementación realizada, procedimientos operativos estándar (SOP) adaptados al entorno institucional, guías de resolución de problemas, procedimientos validados de respaldo y recuperación, matriz de contactos de soporte con niveles de escalamiento, así como certificados de garantía y licenciamiento de los componentes suministrados. Toda la documentación deberá ser entregada en **idioma español**, en **formato físico y digital**, incluyendo versiones editables y no editables, y será objeto de revisión y aceptación por parte del supervisor del contrato.

NOTA: LOS EQUIPOS OFERTADOS DEBEN SER NUEVOS, NO SE ACEPTAN EQUIPOS REMANUFACTURADOS, ESTOS DEBERAN TENER UN (1) AÑO DE GARANTIA.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque. Original de fábrica, sellos de integridad, embalaje antiestático y protección mecánica.

3.3.2 Rotulado. Se debe tener en cuenta la NORMA ISO 7000:2019.

Cada unidad deberá contar con rotulado visible y permanente que incluya como mínimo la siguiente información:

- Número de serie.
- Modelo del equipo.
- Etiqueta interna de inventario institucional.
- Nivel de criticidad asignado.

4 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1 Muestreo. Inspección 100% (control total).

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. Los criterios de aceptación o rechazo de esta especificación técnica se basan en el cumplimiento de los requerimientos establecidos en el presente documento técnico relacionados en los Requisitos Generales.

• Empaque íntegro, sin golpes visibles.

• Serial coincide con guía de despacho.

• Encendido sin errores POST.

• Puertos operativos (link up verificado).

Nota: Rechazo si falla alguno y no se corrige en sitio.

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS

4.2.1 Muestreo. Verificación 100% muestreo y elementos recibidos.

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos. Los criterios de aceptación o rechazo de esta especificación técnica se basan en el cumplimiento de los requerimientos establecidos en el presente documento técnico relacionados en los Requisitos Específicos y métodos de ensayo.

5 MÉTODOS DE ENSAYO.

El presente método de ensayo tiene como finalidad verificar el cumplimiento integral de las especificaciones técnicas establecidas para los appliances, garantizando su correcta instalación, funcionamiento, desempeño y confiabilidad operativa dentro de la infraestructura tecnológica institucional. Se debe tener en cuenta lo siguiente:

- El Ítem 4 de Requisitos Específicos – Implementación hará parte integral del método de ensayo, en razón a que durante esta fase se desarrollarán las actividades técnicas de instalación, configuración, puesta en funcionamiento y verificación operativa de los appliances, garantizando el cumplimiento de las condiciones técnicas establecidas.
- Verificación física y eléctrica (multímetro / UPS log).
- Prueba de puertos: detección enlace y MAC en switch.
- Generación de tráfico controlado (herramienta de test / replay PCAP) para validar capacidad y ausencia de drops.
- Simulación de anomalía (escaneo interno, acceso horario inusual) para confirmar detección en consola.
- Prueba de reinicio controlado y persistencia de configuración.
- En caso de presentarse fallas de funcionamiento, defectos de fabricación, degradación de desempeño o cualquier anomalía atribuible al hardware suministrado durante el periodo de garantía, el contratista deberá realizar la sustitución total del appliance afectado por un equipo completamente nuevo, de iguales o superiores características técnicas a las ofertadas. No se aceptarán equipos remanufacturados, reacondicionados, reparados, repotenciados o de reemplazo tipo “refurbished” bajo ninguna circunstancia. El equipo de reposición deberá ser original de fábrica, proveniente directamente del fabricante, contar con garantía integral y mantener la vigencia de soporte técnico conforme a las condiciones contractuales establecidas.

6 APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.

- Ley 80 de 1993 “por la cual se expide el Estatuto General de Contratación de la Administración Pública” y las demás normas que la modifiquen o aclaren.

- Ley 816 de 2003 “por medio de la cual se apoya a la industria nacional a través de la contratación pública” y las demás normas que la modifiquen o aclaren.

- Ley 1150 de 2007 “por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos” y las demás normas que la modifiquen o aclaren.

- Ley 1341 de 2009 “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.

- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Ley 1437 de 2011 “por la cual se expide el código de Procedimiento Administrativo y de lo Contencioso Administrativo”.

- Ley 1474 de 2011 “por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública” y las demás normas que la modifiquen o aclaren.

- Ley 1564 de 2012, “por medio de la cual se expide el código general del proceso y se dictan otras disposiciones”.

- Ley 1712 de 2014 “por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.

- Resolución 4519 de 2016 “por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, a las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.

- Resolución 2710 de 2017 “por la cual se establecen lineamientos para la adopción del protocolo IPv6” y las demás normas que la modifiquen o aclaren.

- Resolución 4130 2022 “por la cual se expide el manual de contratación y de convivencias” y las demás normas que la modifiquen o aclaren.

- Resolución 7870 de 2022 “Política general de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de los servicios tecnológicos en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional”.

- Decreto 410 de 1971 “por el cual se expide el código del comercio”.

• Decreto 19 de 2012 “por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública” y las demás normas que lo modifiquen o aclaren.

• Decreto 1082 de 2015 “por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional” y las demás normas que lo modifiquen o aclaren.

• Decreto 103 de 2015 “por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones” y las demás normas que lo modifiquen o aclaren.

• Decreto 620 de 2020 "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"

• Decreto 338 de 2022 “Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”

• Directiva de Seguridad de la Información del Ministerio de Defensa 2014-18 “Políticas de seguridad de la información para sector defensa”

• Directiva permanente 00221 de 2017 “Seguridad de la información para el Ejército Nacional”.

• Norma técnica NTC-ISO/IEC colombiana 27001 “Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información. Requisitos”

• Nist.cswp.29.spa El Marco de Seguridad Cibernética (CSF) 2.0 del NIST

• Nist.sp.800-161r1. Prácticas de gestión de riesgos de la cadena de suministro para sistemas de información y organizaciones federales.

APPLIANCES PARA EL MONITOREO Y ANÁLISIS DE TRÁFICO DE RED DE LA UNIDAD DE CIBERDEFENSA DEL EJÉRCITO NACIONAL.	
1	**INSTALACIÓN:**
1.1	**Instalación de los appliances** El contratista junto con el supervisor debe realizar un plan de trabajo para el correcto despliegue de los appliances garantizando la operación y puesta en funcionamiento correctamente. El contratista deberá asumir la totalidad de los costos derivados del despliegue, transporte, instalación, configuración e integración de los appliances objeto del contrato a nivel nacional, en las unidades, sedes o dependencias del Ejército Nacional donde sean requeridos.

	La instalación deberá realizarse garantizando la correcta integración con las tecnologías y la infraestructura tecnológica existente del Ejército Nacional, asegurando su óptimo funcionamiento, interoperabilidad y desempeño en todos los sitios de implementación, sin que ello genere costos adicionales para la Entidad.
1.2	**Instalación y Configuración de los Appliances** Realizar una correcta instalación: Se deberá realizar la correcta instalación, configuración y puesta en marcha de los appliances (sensores de red), siguiendo las recomendaciones técnicas, lineamientos y especificaciones establecidas por el fabricante, así como verificando el cumplimiento de los requisitos de hardware, software y conectividad necesarios para su adecuada operación dentro de la infraestructura tecnológica institucional. Asimismo, se deberá garantizar la correcta integración de los equipos con la red institucional y con las plataformas de monitoreo y seguridad existentes, realizando las pruebas técnicas necesarias para validar su funcionamiento y asegurar su adecuada operación. Los appliances serán instalados en las siguientes ubicaciones estratégicas: 1. Popayán – Cauca 2. Cartago – Valle del Cauca 3. Barranquilla – Atlántico 4. Tunja – Boyacá 5. Bogotá – Bogotá D.C. 6. Bogotá – Bogotá D.C. 7. Maicao – La Guajira 8. Cáceres – Antioquia 9. Yopal – Casanare 10. Medellín – Antioquia Configuración adecuada: La configuración correcta y puesta en marcha de los appliances, debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red. Pruebas de integración: El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de los appliances en la infraestructura existente y asegurarse de que la implementación esté proporcionando el servicio esperado.
1.3	**Entrega de Diagrama Técnico de Red**

	Al finalizar la implementación el contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los appliances con sus correspondientes conexiones de red de dato con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.
1.4	**<u>Caso de Fallas</u>** Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo: • Cambio de equipos en caso de fallas deben contar con software preinstalado de fábrica. • Remplazo de equipos por otros de iguales o superiores características. • Configuraciones, puesta en producción y funcionamiento. En caso de falla, el contratista deberá gestionar ante el fabricante el suministro de los materiales y/o piezas necesarias para la reparación o reemplazo, con características iguales o superiores, sin costo alguno para la Entidad. En caso de presentarse fallas ocasionadas por las actividades efectuadas como producto de la ejecución del contrato por parte del contratista, este debe garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados.
2	**<u>Garantía Técnica</u>** El contratista deberá garantizar una mesa de apoyo para instalación y configuración de los appliances para el registro y seguimiento de los casos reportados por la Entidad, de conformidad con lo requerido en las especificaciones técnica. El fabricante debe contar con línea para atención 24/7. Nota 1: En caso de que los appliances requieran escalamiento a especialistas de fabricante, estos no generarán costos adicionales para la institución y será responsabilidad del contratista la obtención de las soluciones necesarias dentro de los tiempos establecidos.
2.1	**<u>Término de Respuesta de la Garantía Técnica</u>** Para el presente proceso de selección, el contratista deberá presentar el termino de respuesta de la garantía técnica, el cual cubrirá lo siguiente:

	• El soporte se puede realizar remotamente o en sitio de acuerdo con la solicitud del Supervisor del contrato. • Línea de Atención. • El Contratista deberá proveer una línea de soporte y un correo electrónico para que el personal encargado pueda reportar inconvenientes que se presenten con la implementación y configuración de los appliances, con el fin de generar un ticket de servicio y llevar el control del tiempo de atención. • El Contratista deberá garantizar el normal funcionamiento de los appliances después de la instalación y puesta en marcha, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de los appliances en un tiempo no mayor a 24 horas. **NOTA1:** Estarán a cargo del contratista todos los costos en que debe incurrir en el cumplimiento de su deber de garantía. **NOTA 2:** Los términos de garantía técnica y el tiempo de respuesta de la misma, deberán ser aportados en documento independiente debidamente suscrito por el oferente.
3	**RECURSOS HUMANOS**
3.1	Implementación: La implementación debe ser realizada por personal técnico especializado de acuerdo con los siguientes perfiles, por lo tanto, el oferente deberá presentar junto con la oferta los siguientes requerimientos: <u>Líder o gerente del Proyecto:</u> Profesional responsable de coordinar y supervisar la ejecución del contrato, así como de comunicarse con el supervisor del contrato para garantizar el cumplimiento de los objetivos y las obligaciones establecidas, encargado de la implementación de los appliances a adquirir y con quien se gestionarán el cumplimiento del objeto del contrato, debe cumplir con los siguientes requisitos. ✓ Se requiere que el rol **del líder o gerente del proyecto**, la realice como mínimo un (01) ingeniero con el siguiente perfil: - Ingeniero electrónico, ingeniero de sistemas y/o telecomunicaciones, con especialización o maestría en gerencia de proyectos y/o gerencia y gestión de proyectos, con fecha de expedición en tarjeta profesional superior a cuatro (04) años, tarjeta profesional vigente. ✓ Certificado en Scrum Master vigente. ✓ Certificado en ciberseguridad tipo Lead Cybersecurity Professional vigente, emitido por entidades certificadoras reconocidas a nivel nacional o internacional, tales como CertiProf, PECB o EC-Council, el cual deberá encontrarse activo al momento de la presentación de la propuesta,

	garantizando así la idoneidad y competencias del personal en la gestión y protección de la información. ✓ Se verificará la información correspondiente al perfil del ingeniero propuesto (líder) mediante consulta en línea en el sistema del COPNIA, con el fin de validar la autenticidad y estado de su registro profesional. Dicha verificación incluirá la matrícula profesional, su vigencia, estado activo y la inexistencia de sanciones disciplinarias, garantizando que el profesional cumpla con los requisitos legales para el ejercicio de la ingeniería en Colombia. <u>Implementación:</u> Profesional operativo que se encargará de la implementación y despliegue de los appliances a adquirir, configuración e integración con las soluciones con los que cuenta la Fuerza. ✓ Se requiere que la implementación de los appliances, la realice como mínimo uno (01) ingeniero con el siguiente perfil: - Ingeniero electrónico, ingeniero de sistemas y/o telecomunicaciones, con tarjeta profesional vigente superior a cuatro (04) años. Deberá acreditar los siguientes requisitos de experiencia y confirmación de asistencia: ✓ El ingeniero propuesto deberá acreditar experiencia mínima de dos (2) años, acumulada, en administración, configuración, operación y/o implementación de la solución NDR actualmente desplegada en la Fuerza. ✓ Se requiere que el ingeniero propuesto presente confirmación de asistencia de dos (02) cursos vigentes emitidos por el fabricante, relacionados con la solución de monitoreo y análisis de tráfico de red (NDR) ofertada, específicamente Threat Visualizer Administration y Cyber Engineer. ✓ Se verificará la información correspondiente al perfil del ingeniero propuesto (implementador) mediante consulta en línea en el sistema del COPNIA, con el fin de validar la autenticidad y estado de su registro profesional. Dicha verificación incluirá la matrícula profesional, su vigencia, estado activo y la inexistencia de sanciones disciplinarias, garantizando que el profesional cumpla con los requisitos legales para el ejercicio de la ingeniería en Colombia. **Nota1:** Los ingenieros deben ser de nacionalidad colombiana. **Nota2:** El oferente deberá presentar junto con la oferta las hojas de vida con sus respectivas certificaciones académicas y de experiencia laboral en las funciones requeridas para los anteriores perfiles: <u>Para realizar la validación correspondiente del personal requerido, el oferente debe aportar la siguiente documentación del personal encargado de estas actividades.</u>

	✓ Copia legible del diploma de pregrado como ingeniero de sistemas, electrónico, o de telecomunicaciones. ✓ Copia legible de la tarjeta profesional. ✓ Copia legible del diploma de posgrado en el nivel de especialización o maestría en gerencia de proyectos y/o gerencia y gestión de proyectos. ✓ Copia de cédula de ciudadanía que verifique la nacionalidad colombiana. ✓ La experiencia se deberá certificar considerando los siguientes aspectos que se relacionan a continuación: ✓ Nombre o razón social del contratante ✓ Descripción de las actividades realizadas ✓ Fecha de iniciación del contrato ✓ Fecha de terminación del contrato ✓ Dirección y teléfono de quién expide la certificación ***Nota 1: No se aceptan certificaciones con enmendaduras y que no contengan como mínimo la información solicitada o que presenten inconsistencias.*** ***Nota 2: El Comité técnico evaluador, se reserva el derecho de verificar la veracidad de la información suministrada por el oferente.*** ***Nota 3: No se acepta ningún otro documento para acreditar la experiencia. NO SE ACEPTAN AUTO CERTIFICACIONES.*** ***Nota 4: Las copias de los documentos presentadas deben ser completamente legibles.*** Otras obligaciones del contratista: El Contratista, durante la ejecución del contrato, acepta que el Ejército Nacional evalúe el desempeño profesional de la(s) persona(s) asignadas para el proyecto y estará(n) en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del supervisor del contrato. Durante la ejecución del contrato, si se requiere reemplazar un funcionario por otro, éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado, y cumplir con los requerimientos estipulados en esta especificación técnica. En caso de que el contratista requiera realizar un cambio de personal, este deberá informar al supervisor del contrato de tal situación con mínimo 10 días de antelación, anexando la hoja de vida del nuevo funcionario que debe cumplir con las especiaciones requeridas. El supervisor evaluará el desempeño laboral del profesional asignado para el soporte y estará en facultad de solicitar su remplazo si lo considera necesario,

	en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.
4	**OBLIGACIONES GENERALES DEL CONTRATISTA:** • **Confidencialidad de la Información** Deber general de confidencialidad El contratista se obliga a mantener estricta reserva sobre toda la información que obtenga o conozca con ocasión de la ejecución del contrato, incluyendo aquella relacionada con los lugares a los que tenga acceso durante su desarrollo, especialmente cuando dicha información haya sido clasificada o marcada como confidencial. Alcance del secreto profesional La empresa adjudicataria, así como todos los integrantes del equipo de trabajo vinculados al proceso contractual, deberán guardar secreto profesional sobre la totalidad de la información, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, independientemente de su naturaleza técnica, comercial, financiera, operacional o de cualquier otro tipo y del medio o soporte por el que haya sido adquirida, ya sea verbal, escrita, grabada o en cualquier otro formato. En consecuencia, el contratista y su equipo de trabajo están obligados a adoptar todas las medidas necesarias para evitar la divulgación, sustracción, duplicación, alteración, ocultamiento, cesión o enajenación de cualquier dato o información conocida como resultado de la ejecución del contrato. Esta obligación no se extingue con la terminación del contrato, sino que permanece vigente con posterioridad a su finalización. Extensión de las obligaciones al equipo de trabajo Todos los miembros del equipo prestador del servicio deberán tener pleno conocimiento de sus deberes de confidencialidad desde el inicio de la ejecución del contrato. En caso de producirse cambios en la composición del equipo, los nuevos integrantes asumirán de manera inmediata las mismas obligaciones establecidas en el presente ítem. A tal efecto, el contratista se compromete a capacitar e informar oportunamente a su personal sobre dichas obligaciones, asumiendo la responsabilidad que se derive del incumplimiento de las mismas. Suscripción del Acuerdo de Confidencialidad y No Divulgación (NDA)

	Al inicio de la ejecución del contrato, el contratista y todo el personal asignado al proyecto deberán suscribir el Acuerdo de Confidencialidad y No Divulgación (NDA) establecido por el Ejército Nacional de Colombia, mediante el cual se comprometen formalmente a mantener reserva sobre toda la información institucional a la que tengan acceso, tanto durante la vigencia del contrato como con posterioridad a su terminación. • **Propiedad Intelectual** Todos los estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato serán de propiedad del Ejército Nacional, quien podrá reproducirlos, publicarlos y divulgarlos, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos, en cumplimiento de los términos establecidos en la Ley 23 de 1982, modificada por la Ley 44 de 1993 y la Ley 1915 de 2018. En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército. El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa y por escrito del Ejército Nacional. Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere. • **Documentación** El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización. Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de los appliances adquiridos, además se debe especificar: - Los recursos necesarios para la instalación. - Cada uno de los pasos que se deben efectuar. - Los tiempos de ejecución de cada uno de los pasos.

	- Para el desarrollo de la instalación se deberá presentar un cronograma de tareas después de firmada el acta de inicio del contrato. - Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en los appliances. - Informe final donde se describa el total de las configuraciones e implementación de los appliances y procesos realizados en la ejecución del contrato - Entrega de topología - Informe de cada visita, documentando los procedimientos realizados. • **<u>Otros</u>** El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información.
5	**<u>Cumplimiento de Normatividad Gubernamental en Materia de Tics</u>** Todas las soluciones deben ser compatibles con los protocolos IPV4 e IPV6 Los bienes y servicios TICS contemplados en el presente anexo técnico, deben brindar soporte al protocolo de internet versión seis (IPv6) de conformidad con la Resolución 2710 del 03 de octubre de 2017 de MINTIC, que en su Artículo 5. "Contratación", estipula: "A partir de la entrada en vigencia de la presente resolución, todos los procesos de selección que inicien las entidades públicas deberán, desde los mismos pliegos de condiciones o lo que haga sus veces, exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TICS." <u>Cumplimiento Normas Técnicas</u> El Contratista debe cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso: ANSI/TIA-568-E Generic Telecommunications Cabling for Customer Premises (2023). Norma vigente que establece las directrices para el diseño, instalación y administración del cableado genérico de telecomunicaciones en instalaciones de clientes, tanto en cobre como en fibra óptica. ANSI/TIA-568-E.1 Commercial Building Telecommunications Cabling Standard (2023).

	Norma internacional vigente que estipula las condiciones técnicas del cableado de telecomunicaciones para edificaciones comerciales, incluyendo topologías, espacios, rutas y distancias. ANSI/TIA-568-E.2 Balanced Twisted-Pair Telecommunications Cabling and Components (2023). Norma que define y regula las especificaciones técnicas de los componentes de cableado basados en pares trenzados balanceados para infraestructuras de telecomunicaciones comerciales. ANSI/TIA-568-E.3 Optical Fiber Cabling Components (2023). Norma vigente que establece las directrices generales para los componentes de fibra óptica utilizados en sistemas de telecomunicaciones, incluyendo tipos de fibra, conectores y desempeño. ANSI/TIA-607-D Commercial Building Grounding and Bonding Requirements for Telecommunications (2019). Norma que define los requisitos de puesta a tierra y equipotencialidad para sistemas de telecomunicaciones en edificaciones comerciales, con el fin de garantizar seguridad eléctrica y protección de los equipos. ANSI/TIA-526-7-B Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant. Norma vigente para la medición de la pérdida de potencia óptica en plantas de cable de fibra óptica monomodo instaladas. ANSI/TIA-526-14-C Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant. Norma vigente para la medición de la pérdida de potencia óptica en plantas de cable de fibra óptica multimodo instaladas. IEC 61000-5-2 – Electromagnetic Compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 2: Earthing and cabling. Norma internacional vigente que establece directrices para la compatibilidad electromagnética, enfocadas en instalación, puesta a tierra y cableado, con el fin de mitigar interferencias electromagnéticas. ISO/IEC 11801-1:2017 y enmiendas – Information technology – Generic cabling for customer premises. Norma internacional vigente que define el cableado genérico para instalaciones de usuario, alineada con estándares globales de telecomunicaciones. CENELEC EN 50173-1:2018 y enmiendas – Information Technology – Generic Cabling Systems. Norma europea vigente para sistemas de cableado genérico, equivalente y complementaria a ISO/IEC 11801. ANSI/TIA-942-B Telecommunications Infrastructure Standard for Data Centers (2022). Norma vigente que define los requisitos de infraestructura de telecomunicaciones para centros de datos, incluyendo cableado, espacios, rutas, redundancia y puesta a tierra. ISO/IEC 24764:2019 – Generic cabling for data centre premises. Norma internacional vigente que establece directrices para el cableado genérico en instalaciones de centros de datos.

	Reglamento Técnico de Instalaciones Eléctricas – RETIE (vigente en Colombia). Normativa de obligatorio cumplimiento en el territorio nacional para la ejecución de instalaciones eléctricas, conforme a las disposiciones del Ministerio de Minas y Energía. NTC 2050 – Código Eléctrico Colombiano (basado en NEC). Norma técnica colombiana vigente que regula las instalaciones eléctricas de baja tensión y complementa el RETIE. ICONTEC. Normas técnicas colombianas aplicables a la construcción, fabricación y certificación de materiales y equipos eléctricos y de telecomunicaciones. NEMA / NEC (NFPA 70). Normas internacionales de referencia aplicables de manera supletoria en caso de vacíos técnicos en la normativa local, siempre que no entren en conflicto con el RETIE. El Contratista deberá cumplir en su totalidad con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) y garantizar que los productos comprendidos dentro de su alcance cuenten con certificado de conformidad vigente, expedido por organismos acreditados, para los siguientes elementos, entre otros: • Tomacorrientes • Cable eléctrico • Tableros eléctricos • Tuberías y canalizaciones Protecciones eléctricas (interruptores automáticos, breakers y tomacorrientes con supresor de transientes)
6	**SOPORTE PROVEEDOR:** El proveedor deberá garantizar soporte técnico en horario 24x7 (veinticuatro horas al día, siete días a la semana), en sitio y/o remoto, de acuerdo con lo que sea solicitado por el supervisor del contrato, para los appliances de monitoreo de red objeto del mismo. El soporte deberá cubrir las actividades de instalación, configuración, implementación, puesta en marcha y operación, así como la atención y solución de incidentes que se presenten durante la ejecución contractual. En caso de requerirse el reemplazo total o parcial de equipos, módulos, componentes o partes por garantía o disposición del fabricante, el proveedor deberá asumir la totalidad de los costos asociados, incluyendo transporte, desplazamiento, instalación, configuración, integración y demás actividades necesarias en sitio, sin que ello genere costos adicionales para el Ejército Nacional durante la vigencia del contrato.

	Tiempos de respuesta: El servicio de soporte deberá ser atendido en un tiempo máximo de cuatro (04) horas contadas a partir del reporte del incidente por parte del supervisor del contrato. De ser necesario el proveedor deberá enviar personal técnico especializado a sitio en un tiempo máximo de veinticuatro (24) horas. El tiempo máximo permitido para restablecer el servicio es de 4 horas.
7	**SOPORTE FABRICANTE:** Según las especificaciones proporcionadas, el horario de cobertura de soporte por parte del fabricante debe ser 24x7x365, lo que significa que debe estar disponible los 365 días del año, las 24 horas del día, incluyendo días festivos. Esto garantiza que el Ministerio de Defensa Nacional - Ejército Nacional- Batallón de Ciberdefensa y Ciberseguridad pueda recibir asistencia técnica y soporte en cualquier momento, incluso fuera del horario laboral regular. Es obligatorio que todas las condiciones relacionadas con el soporte técnico, cobertura horaria, instalación, configuración, implementación, puesta en marcha, operación y garantía de los appliances de monitoreo de red objeto del contrato, queden expresamente definidas y detalladas tanto en el contrato como en los documentos de garantía. El Fabricante a través del contratista debe incluir los servicios de revisión y validación del estado de salud de los appliances generando informes para optimización y verificación de casos específicos solicitados por el supervisor del contrato.
8	**Personal Técnico Especializado del Contratista** El Contratista deberá contar con personal técnico especializado, debidamente capacitado y certificado, con experiencia comprobada en la implementación, instalación y configuración de los appliances objeto del contrato, garantizando su correcta puesta en marcha, integración con la infraestructura existente y funcionamiento.
9	**Certificación de Fabricante** El oferente deberá adjuntar, como documento independiente dentro de la oferta, una certificación vigente emitida directamente por el fabricante de los appliances, en la cual se acredite que el oferente se encuentra debidamente autorizado como canal certificado para la comercialización, distribución, implementación y soporte técnico de los productos y análisis de tráfico de red. Así mismo, el oferente deberá presentar una carta del fabricante de los appliances, en la cual se avale los appliances y se certifique que estos cumplen con la totalidad de las características técnicas requeridas.

	Adicionalmente, el contratista se compromete a entregar al supervisor del contrato, dentro de los primeros cinco (5) días posteriores a la formalización del contrato, una certificación o documento expedido por el fabricante que respalde la compra de los appliances propuestos.
10	**TRANSFERENCIA DE CONOCIMIENTO**
10.1	El Contratista debe realizar transferencia de conocimiento para cuatro (04) personas, del Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional curso de configuración y instalación de los appliances objeto del contrato, dictado directamente por el canal implementador en la ciudad de Bogotá en instalaciones del BACCI de mínimo 40 horas. **Se debe expedir certificado por parte de fábrica y/o Canal implementador en idioma español**. Temas: ✓ Introducción de los appliances adquirir. ✓ Configuración de los appliances. ✓ Fundamentos de los appliances. ✓ Administración de los appliances. ✓ Mejores prácticas **Nota:** Se debe realizar laboratorios teóricos prácticos del temario.
11	**Aclaración de ítem de la especificación técnica ET-JEMPP-CEDE6-0562.**
11.1	**Ítem 3.2.2.1 "Perfil de capacidad – Tipo 1 (Principal):** De acuerdo con el ítem 3.2.2.1, se precisa que los valores de capacidad se ajustan en función de los parámetros técnicos requeridos para garantizar la adecuada operatividad, interoperabilidad y calidad de los appliance, asegurando un margen de rendimiento óptimo acorde con la necesidad establecida; en consecuencia, este ítem deberá entenderse con una capacidad mínima de 25.000 conexiones por minuto, un throughput efectivo mínimo de 400 Mbps y una capacidad de análisis de hasta 5.000 dispositivos, o capacidades funcionalmente equivalentes o superiores.
11.2	**Ítem 3.2.2.2 "Perfil de capacidad – Tipo 2 (Pro):** De acuerdo con el ítem 3.2.2.2, se precisa que los valores de capacidad se ajustan en función de los parámetros técnicos requeridos para garantizar la adecuada operatividad, interoperabilidad y calidad de los appliance, asegurando un margen de rendimiento óptimo acorde con la necesidad establecida; en consecuencia, este ítem deberá entenderse con una capacidad mínima de 25.000 conexiones por minuto, un throughput efectivo mínimo de 400 Mbps y una capacidad de análisis de hasta 5.000 dispositivos, o capacidades funcionalmente equivalentes o superiores.
11.3	**Ítem 3.2.3.43 "Respuesta autónoma":** De acuerdo con el ítem 3.2.3.43, se precisa que la capacidad de respuesta autónoma ante la detección de un

	incidente anómalo deberá ejecutarse mediante el mecanismo de TCP/Reset, permitiendo interrumpir de manera inmediata la actividad maliciosa identificada y garantizando la continuidad de las operaciones normales de la red, en concordancia con los parámetros de operatividad e interoperabilidad.

El OFERENTE

_____

REPRESENTANTE LEGAL O APODERADO
Nombre Identificación Razón social
C.C. / NIT XXXXXX