REPÚBLICA DE COLOMBIA

PATRIA HONOR LEALTAD

EJÉRCITO NACIONAL DE COLOMBIA

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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: JEMPP-CEDE6-0562 - V0

PÚBLICO

CONTENIDO

1. OBJETO 3
2. DEFINICIONES, CLASIFICACIÓN Y APLICACIÓN 3
3. REQUISITOS 9
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO 34
5. MÉTODOS DE ENSAYO 35
6. APÉNDICE 36
7. ANEXOS 38
8. CONTROL DE REVISIONES 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 PEREZ** 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 AREVALO RIOS** Comandante de la Brigada de Interoperabilidad Computación y Ciberdefensa

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

a los administradores garantizar que, a menos que el dispositivo presente las credenciales adecuadas, no pueda obtener acceso.[1]

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. [2]

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. [3]

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. [4]

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. [5]

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. [6]

---

[1] Fortinet. (2017). Network access control list (NAC).. https://www.fortinet.com/lat/resources/cyberglossary/network-access-control-list
[2] IBM. (2021). What is artificial intelligence? https://www.ibm.com/mx-es/think/topics/artificial-intelligence
[3] Amazon Web Services, Inc. (2011). ¿Qué es AWS?. https://aws.amazon.com/es/what-is-aws/
[4] Amazon Web Services, Inc. (2011). What is RTT in networking?. https://aws.amazon.com/es/what-is/rtt-in-networking/
[5] Fortinet. (2011). What is DNS?. https://www.fortinet.com/lat/resources/cyberglossary/what-is-dns
[6] Google Cloud. (2011). ¿Qué es IaaS? https://cloud.google.com/learn/what-is-iaas?hl=es

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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. [7]

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. [8]

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. [9]

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. [10]

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. [11]

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. [12]

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. [13]

---

[7] Wikipedia. (2009). Comisión Electrotécnica Internacional. Recuperado el 22 de febrero de 2026, de https://es.wikipedia.org/wiki/Comisi%C3%B3n_Electrot%C3%A9cnica_Internacional

[8] Cloudflare, Inc. (2018). ¿Qué es el protocolo de Internet (IP)? https://www.cloudflare.com/es-es/learning/network-layer/internet-protocol/

[9] Amazon Web Services, Inc. (2009). ¿Cuál es la diferencia entre IPv4 e IPv6? https://aws.amazon.com/es/compare/the-difference-between-ipv4-and-ipv6/

[10] Microsoft. (2017). IPv6 overview.. https://learn.microsoft.com/es-es/dotnet/fundamentals/networking/ipv6-overview

[11] International Organization for Standardization. (s.f.). ISO. Recuperado el 22 de febrero de 2026, de https://www.iso.org/es/home

[12] MultiTech Systems, Inc. (2010). Media access control (MAC).. https://multitech-com.translate.goog/iot-wiki/media-access-control-mac/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[13] Amazon Web Services, Inc. (2017). ¿Qué es MFA (autenticación multifactor)? https://aws.amazon.com/es/what-is/mfa/

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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. [14]

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. [15]

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. [16]

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. [17]

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. [18]

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. [19]

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

---

[14] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2009). [Titulo del documento]. https://www.calameo.com/books/0015930041ba5a9cbe0e6

[15] TechTarget, Inc. (2010). Network Time Protocol (NTP). https://www-techtarget-com.translate.goog/searchnetworking/definition/Network-Time-Protocol?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[16] Corelight, Inc. (2012). Packet capture (PCAP). https://corelight-com.translate.goog/resources/glossary/packet-capture-pcap?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[17] TechTarget, Inc. (2017). POST (Power-On Self-Test). https://www-techtarget-com.translate.goog/whatis/definition/POST-Power-On-Self-Test?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[18] Fortinet. (2008). QoS (quality of service). https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service

[19] Amazon Web Services, Inc. (2018). ¿Qué es SaaS (software como servicio)? https://aws.amazon.com/es/what-is/saas/

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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. [20]

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. [21]

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. [22]

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. [23]

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. [24]

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. [25]

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. [26]

---

[20] FiberMall. (2006). ¿Qué es un puerto SFP+? https://www.fibermall.com/es/blog/sfp-plus-port.htm?srsltid=afmboooqhh8x58grbs9tmomb6iamejpfb3wjs7zwsr4q2ia95jed_pmz

[21] Microsoft. (2012). ¿Qué es SIEM? https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem

[22] Amazon Web Services, Inc. (2018). ¿Qué es un acuerdo de nivel de servicio (SLA)?. https://aws.amazon.com/es/what-is/service-level-agreement/

[23] IBM. (2018). ¿Qué es SOAR (security orchestration, automation and response)? https://www.ibm.com/es-es/think/topics/security-orchestration-automation-response

[24] GeeksforGeeks. (2019). Switch port analyzer (SPAN). https://www-geeksforgeeks-org.translate.goog/computer-networks/switch-port-analyzer-span/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[25] CCNA desde Cero. (2019). ¿Qué es un TAP de red?. https://ccnadesdecero.es/que-es-tap-red/

[26] icorp. (2022). ¿Qué es troubleshooting? https://icorp.com.mx/blog/que-es-troubleshooting/

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.
		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:

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.
3.1.2	SOPORTE FABRICANTE	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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.
		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.
3.1.3	SOPORTE CONTRATISTA	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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.
		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.
3.1.4	**DOCUMENTACIÓN**	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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

		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:

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

		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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

		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).

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

	• 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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	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.
3.2.4.3	**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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	garantizar una captura completa sin degradación del rendimiento. 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.
	ACOMPAÑAMIENTO Y RECOMENDACIÓN DE TUNING
3.2.4.4	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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

	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.

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).

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

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.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

- 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

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

CÓDIGO ET: ET-JEMPP-CEDE6-0562 - V0

PÚBLICO

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

6.2 ANTECEDENTES

Omitido.

7 ANEXOS

Omitido.

8 CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
0	Creación especificación técnica APPLIANCES PARA EL MONITOREO Y ANÁLISIS DE TRÁFICO DE RED DEL EJÉRCITO NACIONAL de conformidad con la solicitud radicado N° 2025574029919013 emitido por el BACCI. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza la pluralidad de oferentes. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. El Batallón de Ciberdefensa y Ciberseguridad BACCI en la presente especificación técnica garantiza que fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional.	2026-03-02

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial