REPÚBLICA DE COLOMBIA

PATRIA HONOR LEALTAD

EJÉRCITO NACIONAL DE COLOMBIA

IMPLEMENTACIÓN Y SOPORTE DE EQUIPOS DE SEGURIDAD PERIMETRAL

SUBSISTEMA: Inteligencia y Contrainteligencia			
ESPECIALIDAD: Inteligencia Militar			
PROCESO: Producción de Inteligencia y Contrainteligencia.	**NIVEL DE CLASIFICACIÓN:** Restringido		
Código ET: ET-JEMPP-CEDE2-0881	**Versión:** 0	**Fecha de emisión:** 2026-05-22	**Número de Páginas:** 31

CONTENIDO

Elaboró	Revisó	Aprobó
PD. BENJAMÍN MONTOYA GAITÁN Comité Estructurador **CP. CARLOS EDUARDO CASTELLANOS URREGO** Comité Estructurador	**PD. SINDY VANESSA GOMEZ ORTIZ** Jurídico CAIMI **ST. CARLOS GARDEL MARTÍNEZ** Oficial de Comunicaciones CAIMI **SV. CANO PLAZA EDWIN LEONARDO** Coordinador mesa técnica CEDE2	**CR. WILLIAM TRUJILLO COLLAZOS** Comandante CAIMI **BG. JOSE LUIS ESPARZA GUERRERO** Jefe del Departamento de Inteligencia y Contrainteligencia

1 OBJETO

La presente Especificación Técnica tiene por finalidad el suministro, implementación, licenciamiento y soporte técnico de equipos de seguridad perimetral tipo firewall y balanceadores de quinta generación (NGFW) físicos, con el objetivo de fortalecer la infraestructura tecnológica institucional mediante la actualización y mejora continua de los mecanismos de seguridad informática. El suministro, implementación y soporte se enmarca dentro de una estrategia integral de ciberseguridad orientada a la prevención, detección y neutralización de amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de la información.

A través de esta, implementación y soporte, se busca proporcionar una infraestructura de seguridad moderna y adaptable, que permita responder proactivamente a las amenazas actuales del entorno digital y al mismo tiempo asegurar el cumplimiento normativo, la continuidad operativa y administrativa de la red de datos del Ejército Nacional, con el fin de salvaguardar la seguridad y la información de las unidades que la requieran.

2 DEFINICIONES, CLASIFICACIÓN Y APLICACIÓN

2.1 DEFINICIONES

Firewall[1]: Un cortafuego (del inglés firewall) es una parte esencial de un sistema informático o de una red que está diseñada para bloquear accesos no autorizados mientras permite comunicaciones permitidas. Actúa como una barrera entre redes confiables (como una intranet) y redes externas (como Internet), inspecciona el tráfico que entra y sale, y toma decisiones—permitir, denegar o descartar—según un conjunto de reglas de seguridad configuradas.

NGFW[2]: Next-Generation Firewall o Cortafuegos de Nueva Generación en español. Es un tipo avanzado de firewall que no solo realiza el filtrado tradicional de paquetes (como los firewalls clásicos), sino que incluye funcionalidades más completas para proteger redes frente a amenazas modernas.

---

[1] Palo Alto Networks. (s. f.). ¿Qué es un cortafuegos? Definición de cortafuegos. Recuperado el 2 de septiembre de 2025
[2] phoenixNAP – "What Is Next Generation Firewall?"– phoenixNAP. (2024, 20 de mayo). What is Next Generation Firewall? Recuperado el 2 de septiembre de 2025, de https://www.phoenixnap.com/

NGSG[3]: Next Generation Security Gateway es un dispositivo o sistema que actúa como puerta de enlace de seguridad avanzada, diseñado para proteger redes frente a amenazas modernas. Es similar al concepto de un Next-Generation Firewall (NGFW), pero puede incluir más capacidades integradas, funcionando como un punto central de defensa unificada.

NGTP4: Next Generation Threat Prevention, que en español se traduce como Prevención de Amenazas de Nueva Generación. Es un conjunto de tecnologías y servicios de ciberseguridad diseñado para prevenir amenazas avanzadas como malware, ransomware, exploits, ataques de día cero, y más.

SSD[5]: Una unidad de estado sólido (Solid State Drive, SSD) es un dispositivo de almacenamiento de datos no volátil que utiliza memoria flash, en lugar de componentes mecánicos, para guardar información digital. A diferencia de un HDD, no posee partes móviles, lo que le confiere varias ventajas: acceso más rápido a los datos, menor latencia, mayor resistencia a vibraciones, funcionamiento silencioso y menor consumo energético. Su arquitectura le permite utilizar interfaces como SATA, PCIe y NVMe para ofrecer un alto rendimiento en una amplia variedad de dispositivos, incluyendo computadoras, servidores y equipos portátiles. Asimismo, aunque el costo por gigabyte puede ser mayor y su vida útil está limitada por ciclos de escritura, el uso actual de tecnologías como la nivelación de desgaste y la recolección de basura (garbage collection) mitiga dichos efectos adversos.

AC[6]: La corriente alterna (AC, por sus siglas en inglés) es un tipo de corriente eléctrica en la cual el flujo de electrones cambia de dirección periódicamente. Este tipo de corriente es el estándar para la distribución de energía eléctrica en hogares, oficinas e industrias en la mayoría de los países, debido a su eficiencia para transmitir electricidad a largas distancias.

DC[7]: La corriente continua (DC, por sus siglas en inglés) es un tipo de corriente eléctrica en la que los electrones fluyen en una única dirección constante. A diferencia de la corriente alterna (AC), donde la dirección del flujo cambia periódicamente, la corriente continua mantiene un flujo unidireccional y estable. Es común en dispositivos electrónicos, baterías y fuentes de alimentación.

---

[3] Zscaler. (s. f.). What Is a Next-Generation Firewall? En Zscaler Security Terms Glossary. Recuperado el 2 de septiembre de 2025, de https://www.zscaler.com/mx/resources/security-terms-glossary/what-is-next-generation-firewall?utm_source=chatgpt.com
[4] Enterprise IT World. (s. f.). Defining Next-Generation Threat Protection. Recuperado el 2 de septiembre de 2025, de Enterprise IT World: https://www.enterpriseitworld.com/emerging-cybersecurity-challenges-a-new-threat-landscape/
[5] IBM. (s. f.). ¿Qué es una unidad de estado sólido? Recuperado el 2 de septiembre de 2025, de IBM: https://www.ibm.com/mx-es/topics/solid-state-drives
[6] Institute of Electrical and Electronics Engineers. (s. f.). Alternating current (AC). Recuperado el 2 de septiembre de 2025, de https://ieee.org
[7] Institute of Electrical and Electronics Engineers. (s. f.). *Direct current (DC)*. Recuperado el 2 de septiembre de 2025, de https://ieee.org

Appliance[8]: Un appliance es un dispositivo, ya sea físico o virtual, diseñado para realizar una función específica de manera eficiente y sencilla de administrar. Estos dispositivos suelen estar optimizados para tareas particulares, facilitando su implementación y gestión en entornos tecnológicos.

Servidores On-Premise[9]: Los servidores on-premise son servidores físicos que se instalan y operan directamente en las instalaciones de una empresa o usuario, a diferencia de los servidores alojados en la nube o en centros de datos externos. Estos servidores ofrecen control total sobre el hardware y los datos, pero requieren gestión y mantenimiento local por parte de la organización.

2.2 CLASIFICACIÓN.

Lo componen: sistemas de seguridad perimetral Firewall tipo 1, Firewall tipo 2, Firewall tipo 3, Sistema Balanceador de Carga de Aplicaciones (Application Load Balancer) tipo 4, Sistema de protección contra Amenazas Persistentes Avanzadas para los servicios de correo (ANTI APT) tipo 5, Sistema de protección orientado a la detección, prevención y mitigación de ataques de Denegación de Servicio Distribuido (DDoS) tipo 6, Plataforma centralizada de gestión de seguridad que integra capacidades de Inteligencia Artificial y aprendizaje automático para la administración unificada, correlación avanzada, automatización y prevención proactiva de amenazas cibernéticas en infraestructuras on-premise, híbridas y en la nube (tipo 7), Plataforma de gestión de seguridad tipo Extended Detection and Response (XDR), clasificada como (Tipo 8), que permite la detección, correlación, análisis y respuesta automatizada frente a amenazas avanzadas, mediante la integración de múltiples fuentes de telemetría, inteligencia de amenazas y analítica avanzada, garantizando una protección integral de la infraestructura tecnológica.

2.3 APLICACIÓN

La presente Especificación Técnica deberá ser aplicada como documento orientador y de referencia obligatoria para los procesos de suministro, implementación y soporte de soluciones de seguridad perimetral del Ejército Nacional.

---

[8] Cisco Systems, Inc. (s. f.). What is an appliance? Recuperado el 2 de septiembre de 2025, de https://www.cisco.com
[9] Microsoft Corporation. (s. f.). What is on-premises software? Recuperado el 2 de septiembre de 2025, de https://learn.microsoft.com/en-us/azure/architecture/on-premises

Su aplicación tiene como finalidad facilitar la correcta interpretación e implementación de los requerimientos técnicos, así como apoyar la estructuración de los pliegos de condiciones, los planes de muestreo, los criterios de aceptación técnica y las responsabilidades contractuales entre la entidad y el oferente.

2.3.1 CONDICIONES:

- Establecer lineamientos claros para la definición de requisitos técnicos mínimos y evaluables en los procesos de contratación.
- Facilitar la elaboración de planes de muestreo, pruebas de aceptación y validación funcional de los equipos y soluciones adquiridas.
- Orientar la correcta implementación, configuración y puesta en operación de las soluciones de seguridad perimetral conforme a las mejores prácticas.
- Proporcionar recomendaciones básicas que regulen la interacción técnica y operativa entre la entidad contratante y el contratista durante las fases de suministro, instalación, soporte y mantenimiento.
- Asimismo, cada dependencia interesada en emplear el presente documento deberá considerar y especificar claramente en los pliegos de condiciones aquellos aspectos en los que la norma técnica admite múltiples opciones o configuraciones, tales como:
- Características físicas o técnicas de los equipos, formato appliance físico o virtual, capacidades de almacenamiento HDD o SSD, interfaces de red, redundancia de fuentes AC/DC).
- Parámetros de dimensionamiento y desempeño (throughput, sesiones concurrentes, usuarios soportados, alta disponibilidad, escalabilidad).
- Requisitos de compatibilidad con la infraestructura existente (entornos on-premise, virtualizados o híbridos).
- Consideraciones de operación, administración y soporte (niveles de servicio, tiempos de respuesta, actualizaciones, licenciamiento y soporte local).

Estos aspectos deberán ser comunicados de manera explícita al oferente con el fin de asegurar que la solución propuesta se ajuste a las necesidades operativas, técnicas y estratégicas de la entidad, garantizando la interoperabilidad, eficiencia, sostenibilidad y cumplimiento de los objetivos de seguridad establecidos.

La correcta aplicación de esta Especificación Técnica contribuirá a la estandarización de criterios, la reducción de riesgos técnicos y contractuales y la optimización de los procesos, fortaleciendo así la postura de ciberseguridad institucional.

3 REQUISITOS

3.1 REQUISITOS GENERALES

Se requiere el suministro, implementación, licenciamiento y soporte técnico de equipos de seguridad perimetral tipo firewall y balanceadores de quinta generación (NGFW) físicos. Sistema de seguridad perimetral firewall tipo 1, Sistema de seguridad perimetral firewall tipo 2, Sistema de seguridad perimetral firewall tipo 3, Sistema de seguridad perimetral tipo balanceador de carga de aplicaciones (Application Load Balancer) tipo 4, Sistema de seguridad perimetral de protección contra amenazas persistentes avanzadas para los servicios de correo (ANTI APT) tipo 5, Sistema de seguridad perimetral de protección orientado a la detección, prevención y mitigación de ataques de denegación de servicio Distribuido (DDoS) tipo 6, Sistema de seguridad perimetral tipo plataforma centralizada de gestión de seguridad que integra capacidades de inteligencia artificial y aprendizaje automático para la administración unificada, correlación avanzada, automatización y prevención proactiva de amenazas cibernéticas en infraestructuras on-premise, híbridas y en la nube (tipo 7), Sistema de seguridad perimetral tipo plataforma de gestión de seguridad tipo Extended Detection and Response (XDR), clasificada como (Tipo 8), que permite la detección, correlación, análisis y respuesta automatizada frente a amenazas avanzadas, mediante la integración de múltiples fuentes de telemetría, inteligencia de amenazas y analítica avanzada, garantizando una protección integral de la infraestructura tecnológica.

3.1.1 VISITA TÉCNICA DE CARÁCTER OBLIGATORIO.

Con el propósito de verificar la plataforma tecnológica con la que opera la entidad, así como permitir al oferente validar la infraestructura actual del sistema de seguridad, garantizando la debida armonía, compatibilidad y continuidad en la operación del sistema de seguridad perimetral de la red de datos, se requiere la realización de una visita técnica obligatoria de carácter estrictamente reservado.

Dicha visita deberá llevarse a cabo en cumplimiento de lo dispuesto en la Ley 1621 de 2013 y su decreto reglamentario, y tendrá como finalidad la inspección del datacenter, en consideración a que se trata de una infraestructura crítica que soporta las operaciones del Ejército Nacional de Colombia. En consecuencia, su acceso, permanencia y desarrollo de actividades estarán sujetos a estrictos controles de seguridad y confidencialidad.

En este sentido, deberán observarse de manera obligatoria, entre otros, los siguientes artículos de la Ley 1621 de 2013:

- Artículo 4: Principios de la función de inteligencia y contrainteligencia, en especial los de legalidad, necesidad, proporcionalidad y finalidad.
- Artículo 5: Reserva legal de la información de inteligencia y contrainteligencia.
- Artículo 7: Deber de confidencialidad y protección de la información.
- Artículo 17: Manejo, custodia y clasificación de la información.
- Artículo 18: Acceso a la información bajo estrictos controles y autorizaciones.
- Artículo 19: Protección de archivos, documentos y fuentes de información.

En consecuencia, el personal autorizado para participar en la visita deberá acatar de manera estricta los protocolos establecidos por la entidad, incluyendo la prohibición expresa de tomar fotografías, realizar grabaciones de video o audio, o efectuar cualquier tipo de registro digital o físico dentro de las instalaciones.

Así mismo, previo al ingreso, cada uno de los asistentes deberá suscribir un compromiso formal de confidencialidad o promesa de reserva, mediante el cual se obligan a proteger, salvaguardar y no divulgar la información a la que tengan acceso durante la visita, en concordancia con el marco legal vigente y las políticas institucionales de seguridad de la información.

El incumplimiento de estas disposiciones dará lugar a las acciones legales, penales, disciplinarias y administrativas a que haya lugar, en consideración a la sensibilidad, carácter estratégico y naturaleza de seguridad y defensa nacional de la información, los sistemas y la infraestructura objeto de la visita.

3.1.2 GARANTÍA DE FABRICANTE.

El hardware suministrado tendrá garantía de tres (3) años 7x24 a partir del recibido a satisfacción del objeto contratado por parte del Ministerio de Defensa – Ejército Nacional. Durante el periodo de garantía, el proveedor deberá suministrar todos los repuestos de iguales o superiores características a los originales, sin costo alguno para el Ministerio de Defensa- Ejército Nacional, con el fin de garantizar el correcto funcionamiento de los equipos.

Durante el periodo de garantía, el proveedor se compromete a reparar los equipos y dejarlos en perfecto estado de funcionamiento en un tiempo máximo de 48 horas.

En caso de que la reparación de que un equipo demore más de cuarenta y ocho (48) horas, el proveedor deberá suministrar en forma inmediata uno de iguales o superiores características durante el tiempo que dure la reparación.

3.1.3 CANALES DE DISTRIBUCIÓN Y SOPORTE EN COLOMBIA.

Se debe ofrecer asistencia técnica, respuesta calificada a consultas, aclaración de dudas, sobre el conjunto de hardware, software y servicios integrales de la solución, para todo el personal que el Ejército Nacional haya destinado a este proyecto durante el periodo de la garantía.

Para ello el contratista deberá contar con un centro local de recepción de reportes e incidentes y solicitudes de asistencia técnica.

Tipo de atención: El servicio se prestará de manera presencial y/o remota, mediante el uso de herramientas web en línea, conforme a los tiempos de respuesta establecidos. Para tal fin, el contratista deberá contar con una mesa de ayuda que permita la gestión, seguimiento y control de los casos reportados.

Tiempos de respuesta: El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica, servicio de correo electrónico o en forma remota. Si en el lapso de dos (02) horas después de haber reportado el incidente no se da solución al mismo o el personal en sitio no ha podido solucionar la falla, el contratista deberá enviar personal técnico especializado de respaldo a sitio en un tiempo máximo de dos (02) horas. El tiempo máximo permitido para restablecer el servicio es de veinticuatro (24) horas.

3.1.4 CONDICIÓN Y ORIGEN DE LOS EQUIPOS SUMINISTRADOS.

Todos los equipos suministrados deberán cumplir íntegra y estrictamente con las siguientes condiciones:

- Equipos totalmente nuevos.

Los equipos deben ser nuevos de fábrica, sin uso previo, sin horas de operación, sin activaciones anteriores y no deben haber sido instalados, probados en producción, arrendados, demostrados ni utilizados bajo ninguna modalidad.

No se aceptarán equipos re manufacturados, reacondicionados, refaccionados, reconstruidos, reparados, re potencializados, "refurbished" o equivalentes, aun cuando cuenten con certificaciones del fabricante o terceros.

- Prohibición de re potencialización.

En ningún caso se permitirá el suministro de equipos re potencializados, entendidos como aquellos a los que se les haya reemplazado parcial o totalmente componentes internos (hardware) para extender su vida útil, mejorar desempeño o restablecer funcionalidad.

Esta prohibición aplica tanto a equipos principales y sus componentes como a módulos, tarjetas, fuentes de poder, discos, memorias, licencias, accesorios y repuestos.

- Empaques originales.

Los equipos deben entregarse en sus empaques originales de fábrica, completamente sellados, sin alteraciones, roturas o manipulaciones, e incluyendo:

- Sellos de seguridad del fabricante.
- Etiquetas originales con número de serie, modelo, versión y país de origen.
- Manuales, guías rápidas y documentación original.
- Accesorios originales (cables, soportes, rieles, adaptadores, etc.).
- Trazabilidad y verificación.

Cada equipo deberá contar con número de serie único, verificable directamente en el portal oficial del fabricante.

La Entidad se reserva el derecho de validar la autenticidad, fecha de fabricación, estado y garantía de los equipos directamente con el fabricante o su representante autorizado.

Los equipos deberán contar con garantía oficial del fabricante, vigente a partir de la fecha de aceptación por parte de la entidad.

No se aceptarán garantías de terceros, paralelas o no respaldadas directamente por el fabricante.

- Licencias y software.

El software, firmware y licencias suministradas deberán ser originales, nuevas, sin uso previo, no transferidas ni reutilizadas.

Las licencias deberán entregarse a nombre de la Entidad y permitir el acceso a actualizaciones y soporte oficial durante la vigencia del contrato.

- Derecho de rechazo.

La Entidad podrá rechazar total o parcialmente los equipos que no cumplan con estas condiciones y características técnicas, sin que ello genere costos adicionales.

En caso de detectarse incumplimiento posterior a la entrega, el proveedor deberá reemplazar los equipos de manera inmediata, sin afectar los plazos contractuales.

3.2. REQUISITOS ESPECÍFICOS

Tabla 1. Descripción de requerimientos específicos.

3.2.1	SISTEMAS DE SEGURIDAD PERIMETRAL FIREWALL (TIPO 1.)
	Suministro, instalación y puesta en funcionamiento del firewall en alta disponibilidad con tecnología Maestro, con las siguientes características técnicas mínimas así: unidades de rack: Mínimo una (01) unidad de Rack Cantidad de appliance: Dos Consola de administración: Con las mismas características de la que está instalada actualmente en la infraestructura. Licenciamiento: NGTP Garantía: Directamente con el fabricante. Soporte: 7 X 24 soporte Colaborativo Canal CCSP. Los equipos suministrados deben contar con las siguientes características técnicas mínimas, así:

3.2.1.1	Firewall: Performance: • Throughput 200 Gbps en firewall sobre paquetes UDP 1518 byte • Latencia de 1.85µSec • Throughput 46 Gbps de IPS • Throughput 40 Gbps de VPN sobre cifrado base AES-GCM 1452B [Gbps] • 355.000 conexiones por segundo (sobre 64 bytes) • 7.27M conexiones concurrentes (sobre 64 bytes) • 11 Gbps of Threat Prevention (22 Gbps of Threat Prevention en alta disponibilidad) Highlights: • 14x physycal cores, 20x virtual cores • 1x 960GB SSD SATA storage • 32 Gb memory Ram • Lights-Out-Management card • 1x port management 10/100/1000 base-T Rj45 • 1x port sync 10/100/1000 base-T Rj45 • 1x port console RJ45, USB Type-C console port Network expansión slot options: • 8 x 10/100/1000 Base-T RJ45 2 port card • 4x port 10/25G SPF+, 2 DAC de 25GB para conectividad con Orquestadores Dynamic User-based Policy • Integrates with Microsoft AD,LDAP, RADIUS, Cisco pxGrid, Terminal Servers • Enforce consistent policy for local and remote users on Windows, macOS, linux, Android and Apple los plataforms Network Connectivity: • Total Phisycal and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateways/with virtual systems) • 802.3ad passive and active link aggregation • Layer 2(transparente) and layer 3 (routing) mode

	High Availability: • Active/Active L2, Active/Passive L2 and L3 • Sesión failover for routing change, device and link failure • Cluster XL or VRRP IPV6: • NAT66, NAT64, NAT46 • CoreXL, SecureXL, HA with VRRPv3 Power Requirements: • Dual dc power supplies for 16000 and 23000 appliances • AC power input: 100 to 240V (47-53Hz) • DC input current: -40.5V/24A -48V/19.2A, -60V/16.0A Certifications: • Safety: UL, CB, CE, TUV GS • Emissions: FCC, CE, VCCI, RCM/C-Tick • Environmental: RoHS, WEEE, REACH[1] ISO14001[1] Características técnicas mínimas, así: Highlights: • 48x 10/25GbE and 8x 100GbE • 1.28 Tbps Throughput
3.2.2	**SISTEMAS DE SEGURIDAD PERIMETRAL FIREWALL (TIPO 2.)**
	Suministro, instalación y puesta en funcionamiento del firewall de las mismas características y compatible con la infraestructura actual y la consola de administración, con las siguientes características técnicas mínimas así: Unidades de rack: Mínimo una (01) unidad de Rack Tipo: Appliance Categoria: Branch office and small to medium business security

3.2.2.1	appliance Los equipos suministrados deben contar con las siguientes características técnicas mínimas, así: Performance: • Throughput 25 Gbps en firewall sobre paquetes UDP 1518 byte • Throughput 11 Gbps de IPS • Throughput 5.5 Gbps Threat Prevention • Throughput 5.5 Gbps de VPN sobre cifrado base AES-128 • 75.000 conexiones por segundo • 4.5M conexiones concurrentes • 5 Gbps of Threat Prevention Highlights: • 16 x 1GbE RJ45 • 2 x 2.5GbE RJ45 • 4 x 10GbE SFP+ • 8 x 1GbE SFP Dynamic User-based Policy • Integrates with Microsoft AD, LDAP, radius, Cisco pxGrid, Terminal Servers • Enforce consistent policy for local and remote users on Windows, macOS, linux, Android and Apple los plataforms Network Connectivity: • Total Phisycal and virtual (VLAN) interfaces per appliance: 1024 • 802.3ad passive and active link aggregation • Layer 2(transparente) and layer 3 (routing) mode IPV6: • local network and internet connections, dual stack tunneling IPv4 over IPv6 networks, prefix delegation Power Requirements:

	• two redundant 150W power supplies • 100 – 240VAC, 50 – 60 Hz Certifications: • Safety: CB IEC 62368-1, CE LVD EN62368-1, UL62368-1, ASNZS 62368.1 • Environment: CE, FCC IC, VCCI, ASNZS ACMA • Emissions: ROHS, REACH, WEEE, ISO14001
3.2.3	**SISTEMAS DE SEGURIDAD PERIMETRAL FIREWALL (TIPO 3).**
3.2.3.1	Suministro, instalación y puesta en funcionamiento del firewall de las mismas características y compatible con la infraestructura actual y la consola de administración, con las siguientes características técnicas mínimas. Unidades de rack: Mínimo una (01) unidad de Rack Tipo: Appliance Categoria: Branch office and small to medium business security appliance Características: Los equipos suministrados deben contar con las siguientes características técnicas mínimas, así: Performance: • Throughput 15.5 Gbps en firewall sobre paquetes UDP 1518 byte • Throughput 6.9 Gbps de IPS • Throughput 4.0 Gbps de VPN sobre cifrado base AES-128 • 60.000 conexiones por segundo • 2M conexiones concurrentes • 2.5 Gbps of Threat Prevention Highlights:

	• 2x RJ45 2.5GbE copper LAN ports • 8x RJ45 1GbE copper LAN ports • 1GbE copper/fiber DMZ ports • 1GbE copper/fiber WAN ports • USB 3.0 Type-A port • RJ45 console port • USB Type-C console port Certificaciones: • Safety: CB IEC 62368-1, CE LVD EN62368-1, UL62368-1, ASNZS 62368.1 • Environment: CE, FCC IC, VCCI, ASNZS ACMA • Emissions: ROHS, REACH, WEEE, ISO14001
3.2.4	**SISTEMAS DE SEGURIDAD PERIMETRAL (TIPO 4).** Balanceador de Carga de Aplicaciones (Application Load Balancer).
	Suministro, instalación y puesta en funcionamiento de dos balanceadores de cargas, con las siguientes características técnicas mínimas así: Unidades de rack: Mínimo una (01) unidad de Rack Tipo: Appliance Cantidad de apliance: Dos Características: Los equipos suministrados deben contar con las siguientes características técnicas mínimas, así Procesador: Mínimo Intel Quad-Core o superior, con arquitectura de alto rendimiento adecuada para el manejo intensivo de paquetes y criptografía. Interfaces de red: Mínimo 2 puertos 10 GbE SFP+ y 8 puertos 1 GbE RJ45 para garantizar conectividad flexible y alta capacidad de transferencia.

	Fuente de alimentación: Doble fuente de alimentación redundante, intercambiable en caliente, para garantizar alta disponibilidad y continuidad operativa. Rendimiento de red: ➢ Conexiones simultáneas máximas a nivel L4: al menos 24 millones. ➢ Solicitudes por segundo (RPS) L7: mínimo 290,000. ➢ Conexiones por segundo (CPS) L4: mínimo 183,000. ➢ Operaciones criptográficas RSA con llaves de 2K bits: al menos 7,400 CPS. ➢ Operaciones criptográficas ECC con curva EC-P256: al menos 4,300 CPS. ➢ Capacidad de cifrado SSL masivo: mínimo 3.5 Gbps. ➢ Soporte para crecimiento del throughput hasta 20 Gbps.
3.2.4.1	Instalación y gestión: Soporte para REST API completa que permita crear, leer, actualizar y eliminar configuraciones y objetos, facilitando la automatización y la integración con sistemas de gestión. Seguridad y hardware especializado: Integración con Hardware Security Module (HSM) para la gestión segura de claves criptográficas y aceleración de operaciones criptográficas. Integración con herramientas de automatización y orquestación. Funcionalidades: La solución debe balancear el tráfico enviado desde los clientes a través de la exposición de un servicio virtual y posterior entrega del tráfico a un grupo de servidores reales a balancear. La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Web Application Firewall, para evitar que el balanceador y el WAF compartan los mismos recursos. La solución debe contar con un mecanismo de protección ante ataques de tipo low and slow en TLS

	La solución debe incluir protección contra ataques en capa de aplicación WEB, WAF, y dicho WAF debe estar certificado por ICSA LABS Switching: Mínimo deberá de soportar los protocolos 802.1Q VLAN tagging, Spanning Tree Protocol STP (802.1D), Rapid Spanning, Tree RSTP (802.1w) Multiple Spanning Tree MSTP (802.1s), RIPv1, RIPv2, BGP, OSPFv3. La solución debe incluir un elemento de gestión y control centralizado que soporte la administración y monitoreo de todos los balanceadores/WAF que hacen parte de la propuesta adicionalmente la posibilidad de integrase a la MGMT principal. Acciones de administración: Mínimo deberá dejar aplicar los cambios en la configuración que se hayan realizado, guardar los cambios aplicados, devolver los cambios aplicados, devolver los cambios guardados, comparar los cambios realizados contra la configuración actual. Accesorios: todos los cables y accesorios necesarios para la conexión y configuración del nodo deberán ser suministrados por el contratista
3.2.5	**SISTEMAS DE SEGURIDAD PERIMETRAL (TIPO 5).** Sistema de protección contra Amenazas Persistentes Avanzadas para los servicios de correo (ANTI APT).
3.2.5.1	Se debe realizar la, implementación y puesta en funcionamiento de un Sistemas de seguridad perimetral para la protección de correo y análisis de archivos con las mínimas características técnicas y condiciones que necesita la institución, así: Unidades de rack: Mínimo una (01) unidad de Rack Tipo: Appliance Categoria: Theath Emulation appliance Caraceristicas: Mínimas

	Los equipos suministrados deben contar con las siguientes características técnicas mínimas, así: Performance: • Capacidad de analizar 5000 archivos únicos por hora • Throughput 2.6 Gbps • 28 Virtual Machines Highlights: • 1x 2TB SSD storage • 2x 12 physical, 24 virtual cores • 128 Gb memory Ram • 1x port console RJ45, USB Type-C console port • 2 x 10/100/1000 Base-T RJ45 • 2x port 10 SPF+ with Included 10GbE SR transceivers Certifications: • Safety: UL, CB, CE, TUV GS • Emissions: FCC, CE, VCCI, RCM/C-Tick • Environmental: RoHS, WEEE, REACH[1] , ISO14001[1]
3.2.6	**SISTEMAS DE SEGURIDAD PERIMETRAL (TIPO 6).** Sistema de protección orientado a la detección, prevención y mitigación de ataques de Denegación de Servicio Distribuido (DDoS).
	Se debe realizar la, implementación y puesta en funcionamiento de un sistema de seguridad perimetral con las siguientes características técnicas mínimas y condiciones que requiere la institución, así: Unidades de rack: Mínimo una (01) unidad de Rack Tipo: Appliance Las características mínimas son las siguientes: Arquitectura • Integrar a la red de forma transparente en capa 2.

	• 4 Interfaces de Fibra óptica 10GE Monomodo con su respectivo bypass. • El dispositivo debe incluir al menos dos interfaces de gestión (Management Ports) y administración por consola RJ45. • La solución debe soportar bypass por software para pares de puertos individuales. • La solución de mitigación de ataques DDoS debe soportar la inspeccion de los encabezados internos o externos de tuneles L2TP, GRE, GTP, IPinIP • La solucion debe poder monitorear y alertar sobre el uso de CPU de cada politica definida de forma independiente. • Soportar IPv4 e IPv6 • Soportar un número ilimitado de sesiones concurrentes de ataque. • Doble fuente de poder hot swappable
3.2.6.1	Capacidad • La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 500Mbps por equipo • Soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 20Gbps por equipo • Licenciada para soportar una capacidad de mitigación mínima de 10 Gbps por equipo • Soportar una capacidad de mitigación mínima de 14Millones PPS por equipo • Latencia menor a 60 microsegundos. • La solución de mitigación de ataques DDoS debe incluir hardware dedicado para la mitigación de ataques SSL / TLS con capacidad de al menos 43K CPS con llaves RSA de 2K Funcionalidades de detección y mitigación de ataques La solución debe proteger contra al menos las siguientes anomalías de tráfico: • Checksum incorrecto de IPV4. • Encabezado IPv4 o longitud total invalido. • Tamaño de Encabezado Capa 4 invalido. • TTL igual a 0.

	• Cabecera IPV6 inconsistente. • Límites de salto IPV6 alcanzados. • Protocolo Capa 4 no soportado. • TCP flags invalido. • Dirección de origen o destino igual al Local Host. • Dirección de origen igual a la dirección de destino. • Puerto capa 4 de origen o destino igual a cero. • Cabecera de GRE invalida • Versión GRE Incorrecta • La solución debe operar a través de políticas de seguridad con distintas configuraciones de detección y mitigación de acuerdo a los objetos protegidos. • La solución debe soportar la configuración de dos modos de operación, modo reporte y modo bloqueo. Estos se podrán configurar por política de seguridad y por tipo de protección específica dentro de la política de seguridad. • La solución debe proteger contra ataques de tipo rafaga (burst attacks) identificando que una nueva rafaga de tráfico pertenece a una firma en tiempo real previamente creada. • La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización, debe poder habilitarse a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas: o Bloquear las geografías seleccionadas. o Permitir las geografías seleccionadas. o Permitir las geografías hasta que se supere un umbral determinado por el operador (en PPS o kbps/Mbps " • La solución de mitigación de ataques DDoS debe incluir una lista de IP de mala reputación productos del centro de investigación del fabricante, que será actualizada periodicamente. • La lista de IP debe incluir al menos las siguientes categorías: o Atacantes Activos: Direcciones IP que han sido correlacionados y se han determinado como maliciosas. o Tor Exit Nodes: Una IP que es un Tor Exit Node, sin importar si ha participado o no en actividades de ataques. o Web Attackes: Una IP que ha hecho intentos de ataques Web. o Scanners"

	• La lista de IP maliciosas, en conjunto con las acciones configuradas por categorias, debe aplicarse sobre cada política de seguridad. • La solución debe actuar como un punto de control de feeds, lo que permite gestionar varios feeds y fuentes de datos en un solo lugar. Esto incluye feeds de terceros, listas de bloqueo regulatorias, listas de inteligencia de alta capacidad entre otros. Estas listas pueden ser cargadas usando la interfaz gráfica o de forma automatizada vía API. • Entre otras funcionalidades Consola de Administración • La solución debe incluir un elemento de gestión y control centralizado que soporte la administración y monitoreo de todos los mitigadores que hacen parte de la propuesta y que se integre con la consola actual para el monitoreo de los eventos y correlación de los mismos • El elemento de gestión y control centralizado debe incluir un panel que permita el monitoreo de toda la solución en tiempo real.
3.2.7	**SISTEMAS DE SEGURIDAD PERIMETRAL (TIPO 7).** Plataforma centralizada de gestión de seguridad que integra capacidades de Inteligencia Artificial y aprendizaje automático para la administración unificada, correlación avanzada, automatización y prevención proactiva de amenazas cibernéticas en infraestructuras on-premise, híbridas y en la nube.
	Se debe suministrar una plataforma centralizada de gestión de seguridad que integra capacidades de Inteligencia Artificial y aprendizaje automático para la administración unificada, correlación avanzada, automatización y prevención proactiva de amenazas cibernéticas en infraestructuras on-premise, híbridas y en la nube, con las siguientes características mínimas y condiciones que requiere la institución, así: La solución debe soportar gestión centralizada de seguridad impulsada por Inteligencia Artificial, mediante aplicaciones adicionales (Add-On

3.2.7.1	Applications) integrables sobre plataformas Smart-1 Appliance, Smart-1 Cloud o Management Software, disponibles en el paquete Complete. Requerimientos Funcionales Mínimos 1. Gestión y Análisis de Eventos (SmartEvent) Administración, correlación, análisis y generación de reportes de eventos de seguridad en tiempo real. Capacidad de reportes operativos y de cumplimiento normativo. 2. Prevención Colaborativa y Automatizada de Amenazas (Infinity Playblocks) Orquestación y automatización de respuestas ante incidentes. Prevención colaborativa de amenazas mediante flujos automatizados. 3. Gestión de Identidad y Acceso (Infinity Identity) Control de acceso autenticado bajo modelo Zero Trust. Protección de recursos sensibles mediante identidad centralizada. 4. Optimización y Análisis de Políticas (Policy Insights) Análisis y optimización de políticas de seguridad. Identificación de riesgos y alineación con modelo Zero Trust. 5. Cumplimiento Normativo (Compliance) Verificación de cumplimiento frente a regulaciones y mejores prácticas. Alineación con estándares de seguridad reconocidos. 6. Auditoría de Políticas de Seguridad (Policy Auditor) Validación continua del cumplimiento de lineamientos de seguridad. Detección de desviaciones frente a políticas corporativas. 7. Asistente de Seguridad Basado en IA (Infinity AI Copilot)

	Asistente inteligente para análisis de seguridad. Soporte en investigación de incidentes y toma de decisiones. 8. Monitoreo Preventivo de Infraestructura (Infinity AIOps) Monitoreo proactivo y preventivo de la infraestructura de seguridad. Alertas accionables para gestión del ciclo de vida.
3.2.8	**SISTEMAS DE SEGURIDAD PERIMETRAL (TIPO 8).** Plataforma de gestión de seguridad tipo Extended Detection and Response (XDR).
	Plataforma de gestión de seguridad tipo Extended Detection and Response (XDR), clasificada como (Tipo 8), que permite la detección, correlación, análisis y respuesta automatizada frente a amenazas avanzadas, mediante la integración de múltiples fuentes de telemetría, inteligencia de amenazas y analítica avanzada, garantizando una protección integral de la infraestructura tecnológica.con las siguientes características mínimas y condiciones que requiere la institución, así: Extended Detection and Response La solución XDR (Extended Detection and Response) es una plataforma unificada de detección, correlación, investigación y respuesta automatizada ante amenazas avanzadas, que integra múltiples capas de seguridad (endpoint, red, correo, nube y aplicaciones) bajo un enfoque centralizado, proactivo y basado en inteligencia de amenazas. Alcance de Protección La solución deberá cubrir de forma integral: • Endpoints (Windows, Linux, macOS) • Red perimetral y core (NGFW, IPS, Anti-Bot, Anti-Malware) • Correo electrónico • Nube e infraestructura híbrida • Aplicaciones y cargas de trabajo Capacidades Funcionales Obligatorias Detección Avanzada de Amenazas

	• Detección de malware, ransomware, exploits, ataques fileless y día cero
	• Análisis basado en:
	  ○ Firmas
	  ○ Comportamiento
	  ○ Heurística
	  ○ Machine Learning
	• Integración nativa con ThreatCloud Intelligence

3.2.8.1	Correlación XDR
	• Correlación automática de eventos entre:
	  ○ Endpoints
	  ○ Firewalls NGFW
	  ○ Correo electrónico
	  ○ Tráfico de red
	  ○ Nube
	• Visualización de Kill Chain completa del ataque
	• Reducción de falsos positivos mediante contexto unificado
	
	Respuesta Automatizada (XDR / SOAR-like)
	• Acciones automáticas y manuales:
	  ○ Aislamiento de endpoints
	  ○ Bloqueo de IPs, URLs y dominios
	  ○ Cuarentena de archivos
	  ○ Terminación de procesos maliciosos
	• Playbooks de respuesta configurables
	• Capacidad de respuesta en tiempo real
	
	Protección de Endpoint (Harmony Endpoint integrado)
	• Anti-Malware y Anti-Ransomware
	• EDR con visibilidad completa del endpoint
	• Protección contra exploits de memoria
	• Protección contra ataques sin archivos (fileless)
	• Control de comportamiento de procesos
	• Forense del endpoint (timeline, root cause analysis)
	
	Inteligencia de Amenazas
	• Integración con la plataforma ThreatCloud
	• Inteligencia global en tiempo real

	• Actualizaciones automáticas • Correlación con indicadores de compromiso (IOC) Arquitectura y Despliegue • Soporte para: o On-Premise o Nube o Entornos híbridos • Consola centralizada de administración • Integración nativa con soluciones existentes: o NGFW o Sistema de prevención avanzada contra amenazas persistentes (APT) con sandboxing o Harmony o CloudGuard Gestión y Monitoreo • Consola unificada como se encuentra actualmente. • Dashboards de seguridad en tiempo real • Reportes personalizables: o Incidentes o Tendencias o Cumplimiento • Exportación de logs a SIEM (Syslog, API) Requisitos de Licenciamiento y Soporte • Licenciamiento por: o Endpoint o Gateway o Usuario (según componente) • Actualizaciones de firmas e inteligencia incluidas • Soporte técnico: o 24x7 o Acceso a parches y upgrades • Soporte local o regional autorizado Puede ser la Solución en la nube (Cloud) u Solución On-Premise

Fuente: Comité Especificación Técnica

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque. Todos los elementos que componen sistemas de seguridad perimetral deben ser entregados debidamente envueltos en film plástico elástico (película plástica) tipo industrial, sin embargo, el contratista debe garantizar el empaque necesario y adecuado, de tal forma que ningún componente sufra daños o deterioros durante el transporte y/o almacenamiento. Se debe tener en cuenta que estos componentes no deben presentar rayones, quebraduras, manchas, golpes o roturas.

Todos los elementos que componen el sistema de seguridad deberán llegar en sus empaques originales de fábrica y en excelente estado físico.

3.3.2 Rotulado. Cada componente que conforma la solución de seguridad perimetral debe llevar sus respectivas etiquetas de fábrica debidamente grabadas con impresión de difícil borrado y etiqueta de difícil desprendimiento, el rotulado debe ser claro, legible, teniendo en cuenta las normas técnicas NTC, normas internacionales, reglamentación técnica y boletines SILOG N°5-A1 y SILOG N°5-A2 referentes a la identificación y clasificación del producto. Cada equipo debe llevar el rótulo con la siguiente información:

- Número y fecha del contrato
- Nombre y país del fabricante
- Nombre y país del proveedor
- Número de modelo, serie y subserie
- Nombre del producto
- Unidad de medida: Unidad (C/U)
- Peso
  Fecha de fabricación
- Lote de Fabricación
- Número de serie de fabricación del equipo
- Recomendaciones de Uso
- Recomendaciones de Almacenamiento
- Reglamentación técnica a la identificación y clasificación del producto

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. Sobre todos los firewalls, se debe realizar una inspección visual para verificar si cada elemento cumple con los requisitos generales y requisitos de empaque y rotulado. Se deben verificar los componentes relacionados en el numeral 3.1 REQUISITOS GENERALES del presente documento en su totalidad

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. Si algún elemento llega con cualquier novedad, que afecte las condiciones óptimas de calidad, o que a simple vista se evidencien defectos como: (deterioro, golpes, raspaduras, sucios o en mal estado. Etc). Será objeto de verificación para aceptar o rechazar el lote.

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

4.2.1 Muestreo. Sobre todos los elementos, se debe realizar una inspección para verificar si cada elemento cumple con los requisitos específicos. Se deben verificar los componentes relacionados en la Tabla 2 del numeral ítem No. 3.2.1 No. 3.2.2. No. 3.2.3. No. 3.2.4. No. 3.2.5. No. 3.2.6. No. 3.2.7. No. 3.2.8.

4.2.2 Criterios de aceptación o rechazo para requisitos específicos pruebas de recepción: Para verificar los requisitos específicos de la presente especificación se debe cumplir con el cien por ciento (100%) de lo establecido en la Tabla 2 del numeral 3.2 requisitos específicos mediante la verificación de su funcionamiento y mediante el método de inspección establecido en el numeral 5. métodos de ensayo, de la totalidad de sus componentes. Cuando no se cumpla el criterio de aceptación se rechazará el componente que no cumpla con los criterios establecidos.

Para verificar la correcta instalación y configuración de cada uno los equipos y licencia adquiridos relacionados en los ítems No. 3.2.1 No. 3.2.2. No. 3.2.3. No. 3.2.4. No. 3.2.5. No. 3.2.6. No. 3.2.7. No. 3.2.8., de la presente Especificación Técnica, se procederá a la realización de las pruebas de funcionamiento del sistema de seguridad con acompañamiento del supervisor del contrato.

5 MÉTODO DE ENSAYO

Se llevarán a cabo pruebas funcionales a los equipos suministrados, con el fin de verificar y garantizar la integridad y el cumplimiento de las especificaciones técnicas

requeridas para el equipo, su correcto funcionamiento y la calidad del producto de acuerdo a los parámetros establecidos.

APÉNDICE

6.1. NORMAS QUE DEBEN CONSULTARSE

- Código de procedimiento Administrativo y de lo Contencioso Administrativo Ley 80 de 1993 "por la cual se expide el Estatuto General de Contratación de la Administración Pública" y demás normas que le modifiquen o aclaren.
- Ley 1150 de 2007 "por La cual se expide se introducen medidas para la eficiencia y transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales.
- 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 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 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 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".
- Ley 1437 de 2011 Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".
- Decreto Ley 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.
- Ley Estatutaria 1621 de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, 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.
- Decreto 1070 de 2015 Sector Administrativo de Defensa "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa".
- Directiva permanente radicado No. 20252280106401O3: MDN-COGFM-COEJC-SECEJ-JEMPP-CEDE6-DIPIC-23.1 del 16 de junio de 2025.

6.2 ANTECEDENTES

Para la elaboración de la presente Especificación Técnica no se identificaron normas técnicas, especificaciones técnicas u otros documentos que hayan sido utilizados como base en un porcentaje igual o superior al sesenta por ciento (60%) del contenido del documento. En consecuencia, la estructuración se realizó a partir de análisis técnico propio, revisión normativa aplicable, evaluación de necesidades institucionales y buenas prácticas en la materia, sin que exista un antecedente documental que cumpla con el criterio establecido para su inclusión en este apartado.

7. ANEXOS

Para la presente Especificación Técnica no se incluyen documentos o gráficos anexos, en razón a que las características del elemento, así como los requisitos técnicos, operativos y funcionales, se encuentran descritos de manera integral y suficiente dentro del cuerpo del documento. En consecuencia, no se requiere la incorporación de información complementaria adicional para su comprensión, aplicación o verificación.

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
	Se elabora la presente Especificación Técnica para la adquisición del sistema de seguridad perimetral. Para las unidades del Ejército Nacional, según radicado No. 20265300005195 62 de fecha 10 de abril de 2026 emitido por el CAIMI.	

0	El Comando de apoyo para el Combate para la Inteligencia Militar, en la presente Especificación Técnica, bajo los principios de pluralidad, trasparencia, y de acuerdo a las fuentes relacionadas concluye que las mismas permiten la pluralidad de oferentes, una vez evidenciados los requisitos técnicos general y específicos necesarios para satisfacer las necesidades del Ejército Nacional. El Comando de Apoyo para el combate para la Inteligencia Militar, certifica y garantiza que las características técnicas e información técnica consignada en la presente Especificación Técnica obedecen a una investigación detallada y satisface las necesidades del Ejército Nacional. El Comando de Apoyo para el combate para la Inteligencia Militar, garantiza que este documento técnico fue elaborado de manera profesional, con la mayor trasparencia, siempre buscando enaltecer el nombre del Ejército Nacional.	2026-05-22