ANEXO ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

Facatativá XX de XXXXX de 2024

(El apoderado o representante legal), obrando en nombre y representación de conformidad con lo establecido en el Pliego de Condiciones Definitivo del proceso XXXXXX, ofertó de forma irrevocable, los siguientes bienes o servicios objeto del presente proceso de contratación, con las siguientes características técnicas:

Para efectos de establecer las especificaciones técnicas del presente proceso, cuyo objeto es la **"PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL"** de acuerdo con la especificación técnica No. JEMPP-CEDE6-DIPCO–ET-05524-COM–04, la cual contiene los parámetros técnicos que deben cumplir los oferentes y el contratista en la acreditación de la adquisición del bien, así mismo, el contenido es el mismo del ANEXO ESPECIFICACIONES TÉCNICAS los cuales se describen a continuación:

3.1.1 REQUISITOS GENERALES

La Fuerza a través de su Red Nacional de Datos brinda servicios informáticos desde el Comando del Ejército de forma centralizada, algunos de estos consultados desde internet, por tal razón es fundamental garantizar la operatividad de las herramientas y plataformas evitando accesos no autorizados a la red y así evitar caídas de los servicios críticos a nivel web en el Comando del Ejército y a nivel nacional para todas la Unidades Militares conectadas en Red.

3.1 REQUISITOS GENERALES

<table>
<tr><td>3.2.1</td><td colspan="2">LICENCIAMIENTO</td></tr>
<tr><td>3.2.1.1</td><td colspan="2">ALCANCE:

El proveedor debe brindar el licenciamiento de la solución y debe tener el modelo de licenciamiento por suscripción. El Licenciamiento debe ser entregado al Ejército Nacional para los siguientes productos.

<table>
<tr><th>item</th><th>Descripción</th></tr>
<tr><td>1</td><td>Next Generation Threat Prevention and Sandblast for Additional Appliance</td></tr>
<tr><td>2</td><td>Mobile Access Blade unlimited</td></tr>
<tr><td>3</td><td>Virtual Systems package</td></tr>
<tr><td>4</td><td>Security- browser extension security service.</td></tr>
<tr><td>5</td><td>Internet Access - Essentials package</td></tr>
<tr><td>6</td><td>Cloud Edge Gateway</td></tr>
<tr><td>7</td><td>Collaborative Enterprise Support</td></tr>
<tr><td>8</td><td>Collaborative Enterprise Support - Standard Add-on for Products</td></tr>
</table></td></tr>
<tr><td>3.2.1.2</td><td colspan="2">El proveedor deberá rendir un informe en donde certifique la funcionabilidad de la plataforma, la instalación de las licencias y el no sub-licenciamiento, con sus respectivos soportes; así mismo entregará los certificados de las licencias al Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional.</td></tr>
<tr><td>3.2.2</td><td colspan="2"><u>HARDWARE</u></td></tr>
<tr><td rowspan="8">3.2.2.1</td><td rowspan="8">Appliance de Balanceo y orquestación maestro</td><td><u>Características Hardware</u></td></tr>
<tr><td>Capacidad orquestación Firewalls Mínimo 10 Firewalls</td></tr>
<tr><td>Alta disponibilidad</td></tr>
<tr><td>Performance Máximo 900 Gbps</td></tr>
<tr><td>4 Puertos de 40GB respectivos SFP</td></tr>
<tr><td>4 Puertos de 10GB respectivos SFP</td></tr>
<tr><td>4 Puertos 1G RJ-45 respectivos SFP</td></tr>
<tr><td>4 Puertos de 100GB respectivos SFP</td></tr>
</table>

		Cableado de orquestación para la integración de 4 firewall de seguridad.
3.2.2.2	Firewalls Seguridad de nueva generación	**Características Hardware**
		Throughput Threat Prevention: Mínimo 17 Gps
		2 puertos de 100 GB respectivos SFP
		2 puertos de Gestión Base 10/100/1000 respectivos SFP
		Mínimo 30 millones de conexiones concurrentes por segundo
		Memoria RAM de 128 GB
		Mínimo 8 Grupos de Seguridad
3.2.2.3	Administración & Reportes	**Características Hardware**
		Tipo Appliance (Propietario)
		Procesamiento Logs x seg 40.000 GBS por días de LOGS 600GB
		Almacenamiento 24 TB
		Cantidad Firewall Administrados 40 físicos y/o Virtuales
		Dos unidades de rack
		Doble fuente de poder
		Memoria 192 GB
3.2.2.4	El proveedor deberá incluir para la ejecución del contrato los patch cord OM3 multimodo o ETHERNETUTP y los módulos a 10G o Módulos RJ .5 (point five) que se requieran según la topología propuesta para la solución así: • Deberá realizar las conexiones que se requieran entre racks, con tendido en fibra óptica multimodo OM3 o superior, aplicando la tecnología de cassettes MTP MPO FHD, de acuerdo a lo anterior, el proveedor deberá suministrar todos los elementos pasivos que se requieran para garantizar el funcionamiento de los equipos adquiridos, conservando las buenas prácticas de instalación en centro de cómputo del Ejército Nacional (Las instalaciones de la fibra óptica deben quedar funcionales en su comunicación entre racks o dispositivos que lo requieran) • Deberá realizar las conexiones que se requieran entre racks, de cableado estructurado del centro de cómputo del Ejército Nacional garantizando la correcta operatividad del sistema; Lo anterior deberá quedar claramente rotulado, organizado, certificado y documentado, conservando las buenas prácticas de instalación en el centro de cómputo del Ejército Nacional avalado por el supervisor del contrato. • Adecuación de las conexiones eléctricas (AC) si fuese necesario para la instalación y correcto funcionamiento en el centro de cómputo del Ejercito Nacional. • Verificar el óptimo funcionamiento de las instalaciones eléctricas, de ser necesario se realizará la instalación, renovación o cambio de circuitos o tomas en el centro de cómputo del Ejercito Nacional. • Los equipos activos a implementar en la solución cuentan con doble fuentes de poder, teniendo en cuenta lo anterior se requiere que cada fuente se alimente de circuitos independientes, tomados desde la UPS del centro de cómputo, lo cual garantizara un respaldo eléctrico a los equipos. No se aceptan equipos con sus dos fuentes de poder conectados al mismo circuito. • Suministrar la cantidad de puertos Ethernet y Fiber Channel LAN/SAN, gigabits, fibra óptica y demás elementos necesarios para la puesta en funcionamiento de las soluciones. • Deberá contemplar todos los elementos necesarios para mencionada adecuación sin que genere costos adicionales para el Ejército Nacional. • El Rackeo de las maquinas debe incluir	

	○ Instalación física en el centro de cómputo principal. ○ Adecuación de las conexiones eléctricas si fuese necesario. ○ Configuración software y demás herramientas necesarias para su correcto funcionamiento. ○ Configuración de red: conectividad IP. ○ Movimiento de los equipos que sea necesario reacomodar. ○ Cableado estructurado.
3.2.3	**CARACTERÍSTICAS DE PROTECCIÓN**
3.2.3.1	Firewall y Control de aplicaciones.
3.2.3.2	Soportar stateful inspection, tener predefinidos servicios que abarquen puertos y protocolos de red.
3.2.3.3	Las reglas deben unificar objetos IPv4 e IPv6, soportando NAT 64, NAT 66.
3.2.3.4	Las reglas deben permitir el uso orígenes y destinos basados en países o regiones, permitiendo bloquear o permitir accesos basados en geopolítica.
3.2.3.5	El firewall debe cargar objetos que representen de forma dinámica, direcciones IP, dominios, URLs, que permitan el accesos a sitios de video conferencia (ZooM, Webex, etc), Servicios de Nube (AWS, Azure, Oracle), Compartir Archivos (Box, Dropbox).
3.2.3.6	Debe soportar vía API, lograr integraciones con infraestructura de nube pública y nube privada, para poder construir políticas basadas en etiquetas/tags.
3.2.3.7	Desde la consola de gestión de políticas debe ser posible controlar el acceso desde y hacia determinadas direcciones IP, a través de importar archivos vía Web.
3.2.3.8	La solución debe proveer una herramienta, que ayude aprobar el control de cambios por parte de los administradores de la plataforma, el administrador tendrá un reporte grafico del cambio y El podrá aprobar o rechazar el requerimiento.
3.2.3.9	Debe ser posible definir subpoliticas (ej. Acceso vpn usuarios, acceso a bases de datos) y asignarlos a administradores predeterminados, que tengan gobierno sobre reglas específicas.
3.2.3.10	En cada regla de acceso debe ser posible definir puertos, protocolos, aplicaciones, urls o categorías, o una combinación de las anteriores.
3.2.3.11	Las reglas deben tener la capacidad, de involucrar usuarios/grupos de usuarios que provengan del Directorio Activo de la organización.
3.2.3.12	Debe contarse con la capacidad de ofrecer un agente que evite la suplantación sobre maquinas específicas. Lo anterior significa que a pesar que pueda suplantarse una máquina de un usuario, el agente brindara un factor adicional de validación.
3.2.3.13	Para evitar la evasión en el acceso, debe ser posible involucrar aplicaciones a nivel de internet o servicios internos en la entidad, esto permitirá que acceso a las bases de datos no dependan solamente del puerto que se usa.
3.2.3.14	Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo
3.2.3.15	La solución debe soportar mínimo 8000 aplicaciones explícitamente reconocidas, son de extrema relevancia la contención de aplicaciones tipo proxy (Anonymizers) y categorías riesgosas como las que permiten la fuga/perdida de información (ej. Aplicaciones de repositorios de información)
3.2.3.16	Debe posibilitar la diferenciación y control de partes de las aplicaciones por ejemplo Facebook chat y bloquear Facebook File-Sharing.
3.2.3.17	Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping).
3.2.4	**SISTEMA PREVENCIÓN DE INTRUSOS**
3.2.4.1	La solución debe proveer un componente para identificar y controlar las vulnerabilidades hacia los aplicativos y servicios a través de un módulo de IPS. Este debe manejar mínimo 7000 firmas predeterminadas para el control de este tipo de tráfico.
3.2.4.2	El módulo IPS debe poseer una clasificación alineada a la severidad, nivel de certeza e impacto de las firmas.
3.2.4.3	El módulo de IPS debe proteger a la entidad frente a técnicas de DNS Tunneling
3.2.4.4	El módulo IPS debe prevenir ataques genéricos aun sin la presencia de firmas predeterminadas.
3.2.4.5	El módulo IPS debe controlar el uso no correcto de los protocolos que puedan conllevar actividad maliciosa.

3.2.4.6	La solución debe proveer un mecanismo de actualización de firmas de forma automática, previniendo la carga administrativa de los operadores.
3.2.4.7	El IPS debe ayudar a identificar de forma rápida productos y vendedores a los cuales aplicarles las protecciones
3.2.5	**Filtrado URL**
3.2.5.1	La solución debe permitir categorizar y filtrar los sitios web HTTPS si no está habilitada la inspección HTTPs, por seguridad y evitar un evasiones y bypass de seguridad, la categorización del sitio debe basarse en el contenido del campo SNI enviado en el TLS Client Hello y en el contenido del certificado presentado en el TLS Server Hello
3.2.5.2	El componente de Filtrado debe poseer mínimo 60 categorías, con una base de datos de minimo200 millones de URLs
3.2.5.3	La solución debe categorizar aplicaciones y URLS y adicionalmente debe también soportar aplicaciones por factor de Riesgo.
3.2.5.4	La solución debe incluir listas blancas y negras para permitir al administrador denegar o permitir URLS específicos independientemente de la categoría.
3.2.5.5	La solución debe proveer un mecanismo que sobrescriba la categorización de la base de datos de URL
3.2.5.6	La política de control de aplicaciones y filtrado de URL deben contar con mecanismo de conteo de conexiones sobre cada regla.
3.2.5.7	La solución debe incluir un mecanismo que, al bloquear, preguntar o informar al usuario, en tiempo real presente una página que notifique al usuario la acción tomada, educarlo o confirmar sus acciones de acuerdo con una política de seguridad.
3.2.5.8	Debe permitir la personalización de la página de notificación al usuario indicada en el punto anterior
3.2.5.9	Debe permitir la opción de Safe Search sobre el Gateway para habilitar un mecanismo seguro de las búsquedas sobre los navegadores.
3.2.5.10	Debe soportar una cache local de URL, evitando la demora de comunicación/validación de las URLs a categorías.
3.2.6	**PROTECCIÓN DNS**
3.2.6.1	Debe garantizar la protección y prevención de las comunicaciones de comando y control C2 y prevenir el robo de datos a través de ataques de DNS Tunneling.
3.2.6.2	Debe garantizar protección contra ataques DGA Malware, Bloqueando las conexiones a dominios maliciosos creados a través de algoritmos de generación de dominios (DGA).
3.2.7	**CONTROL DE PHISHING CONOCIDO / DESCONOCIDO**
3.2.7.1	La solución debe controlar el phishing conocido y de día cero. Es decir, a través de un análisis por machine Learning de los diferentes sitios web, en tiempo real.
3.2.7.2	El componente de control de phishing debe poder garantizar que cualquier sitio web que posea un formulario, será bloqueado si este es un sitio que comprometa la información del usuario.
3.2.7.3	El componente de control de phishing deberá contar con la posibilidad de vigilar el uso de las credenciales del dominio del ejército nacional.
3.2.7.4	La solución debe incorporar análisis de mínimo 200 indicadores para conocer si el sitio es engañoso para los usuarios (reputación del dominio, reputación del desarrollador, similitud de iconos/logos con sitios de buena reputación, etc)
3.2.8	**CONTROL DE DATA**
3.2.8.1	En el caso de tráfico que lleve datos, ejemplo tráfico ftp que lleve archivos word, excel, pdf, etc el firewall deberá tener la capacidad de identificar, permitir o bloquear la información de acuerdo con las políticas de seguridad.
3.2.8.2	Para evitar la fuga de información, la solución debe identificar mínimo 500 tipos de datos (ej. archivos comprimidos, archivos de bases de datos, hojas de cálculo, queries SQL, llaves ssh, etc).
3.2.8.3	Permitir identificar y prevenir subida o descarga de información sensible, incluyendo, mas no limitando al número de tarjetas de crédito, certificados digitales, código de programación, permitiendo la creación de nuevos tipos de datos vía expresión regular, palabras clave; identificados sobre aplicaciones a través de HTTP,HTPS, FTP, SMTP.
3.2.9	**CONTROL DE MALWARE CONOCIDO Y DESCONOCIDO**
3.2.9.1	Soportar la inspección y prevención por tipo de archivos, para mínimo 70 clase de ellos

3.2.9.2	Permitir la inspección en archivos comprimidos (zip, gzip, etc.)
3.2.9.3	La solución debe tener la capacidad de detectar y prevenir comunicaciones de comando y control (C&C) de bots informáticos.
3.2.9.4	Permitir el detectar y prevenir el acceso hacia sitios de comando y control (anti-bot), para al menos, dominios, URL, Dirección IP que sean maliciosos.
3.2.9.5	Busque patrones de tráfico C & C, no solo en su destino DNS.
3.2.9.6	Los eventos deben identificar el país de donde partió la amenaza.
3.2.9.7	Garantizar que la solución es capaz de remediar el paciente cero en ataques de malware, es decir se debe garantizar que el primer ataque desconocido no pase.
3.2.9.8	Soportar mínimo el análisis de archivos en el ambiente controlado(sandboxing) del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), flash; archivos ejecutables, DLLs, ZIP y HTTPS.
3.2.9.9	Soportar sandboxing de archivos de mínimo 10 MB tamaño, para todos los tipos soportados
3.2.10	**VIRTUALIZACIÓN**
3.2.10.1	La solución de seguridad ofertada debe estar en la capacidad de virtualizar firewalls, cables, switches y routers
3.2.10.2	La solución debe tener la capacidad de crear mínimo 25 Firewall virtuales, por propósitos de segmentación
3.2.10.3	Cada Firewall virtual debe su propio stack TCP/IP.
3.2.10.4	Los Firewalls virtuales dentro de la solución requerida, deben tener la capacidad de trabajar en modo activo – activo.
3.2.10.5	Cada Firewall Virtual debe tener la capacidad de tener activas las funcionalidades de: • Firewall • Control de Aplicaciones • IPS • Control de Malware Conocido • Control de Malware Desconocido • Filtrado de URLS • Control de Datos • VPN • Seguridad DNS • Phishing Conocido y Desconocido.
3.2.11	**ESCALABILIDAD**
3.2.11.1	La solución debe permitir hiperescalabilidad.
3.2.11.2	La solución brindada no debe ser tipo chasis.
3.2.11.3	La solución debe está compuesta por dos 2 firewalls físicos que se puedan orquestar de manera central, pero con la capacidad de agregar a futuro mínimo 10 equipos adicionales.
3.2.11.4	Debe asimismo garantizar la presencia de dos elementos de orquestación, encargado del balanceo de tráfico, manejo de conexiones e interconexión de los appliances que compongan el Clúster.
3.2.11.5	Cada equipo Firewall de Nueva generación del sistema, debe estar en la capacidad de soportar 16 Gbps en modo Threat Prevention (Firewall, IPS, Filtrado de URL, Control de aplicaciones, Control de Malware Conocido y Desconocido, activados al mismo tiempo).
3.2.11.6	Al agregar cada Firewall adicional del mismo tipo, la solución debe crecer linealmente en su desempeño.
3.2.11.7	A nivel de administración de políticas, el clúster es representado por un único objeto, sin importar el número de Firewalls que compongan la solución.
3.2.11.8	La solución debe garantizar que se prestara el servicio a través de 4 interfaces de 40G, 4 interfaces de 10G en Fibra, y 4 interfaces 1G RJ-45.
3.2.12	**VPN**
3.2.12.1	A cada usuario se le debe asignar una dirección IP diferente, que ayude a la trazabilidad de eventos, y que también permita de forma interna realizar labores de mantenimiento si es requerido (ej. Accediendo vía RDP)
3.2.12.2	Los usuarios deben autenticarse contra el directorio activo de la entidad
3.2.12.3	La solución de VPNs IPSEc debe soportar: Algoritmo Internet Key Exchange (IKEv1 & IKEv2

3.2.12.4	La solución debe soportar Encripcion con AES -128, AES-256 (Advanced Encryption Standard), 3DES
3.2.12.5	Permitir múltiples factores de autenticación para las VPNs client-to-Site IPSEC, con factores propios de autenticación como la combinación Usuarios-password+ One time password(OTP), Certificado digital+Usuarios y password, o traves de la integracion con 3ros fabricantes
3.2.12.6	La solución debe soportar VPNs IPSEC Site-to-Site
3.2.13	**GESTIÓN DE LA SOLUCIÓN DE SEGURIDAD.**
3.2.13.1	La solución debe ser tipo appliance del mismo fabricante, con un almacenamiento mínimo de 14TB.
3.2.13.2	La consola de políticas deberá soportar el acceso de múltiples administradores de forma simultáneos, todos con la capacidad de realizar cambios (no perfil de lectura)
3.2.13.3	La consola debe permitir el gobierno de reglas y políticas a usuarios específicos, es decir el administrador1 puede gestionar las políticas relacionadas a las bases de datos, el administrador 2 gestión de los servidores de almacenamiento, etc.
3.2.13.4	La consola debe ser el punto central para administrar de los firewalls virtuales que se desplieguen en la solución de hiperescalabilidad.
3.2.13.5	El usuario debe poder generar reglas que involucren políticas objetos IPv4 e IPv6 de forma simultánea.
3.2.13.6	La consola debe estar en la capacidad de administrar los firewall existentes físicos y virtuales, si este se extiende a la nube pública (ej. Azure, AWS) o privada (Vmware ESX, Hyper-V)
3.2.13.7	Debe ser posible para el administrador ingresar los (indicadores de compromiso) en forma de archivos tipo CSV
3.2.13.8	La solución debe garantizar la generación de reportes periódicos para la entidad
3.2.13.9	La gestión debe permitir la correlación de eventos de seguridad para conocer el número de incidentes en tiempo real
3.2.13.10	La solución debe brindar la capacidad de analizar los incidentes basado en el framework de Mitre Att&ck
3.2.13.11	La solución debe tener la capacidad de administrar hasta 30 firewall físicos o virtualizados.
3.2.13.12	La solución debe estar en la capacidad de correlacionar eventos, presentar vistas gráficas y generar reportes.
3.2.13.13	Los reportes y vistas deben poderse modificar para alinearse con las necesidades del Ejercito Nacional.
3.2.14	**PREVENCIÓN INTEGRAL DE AMENAZAS PARA USUARIOS WEB**
3.2.14.1	La solución debe brindar acceso sin cliente y confianza de día cero a cualquier aplicación corporativa, desde cualquier navegador web.
3.2.14.2	La solución debe brindar, una experiencia de navegación de Internet segura, rápida y capaz de inspeccionar el 100 % del tráfico SSL.
3.2.14.3	La solución debe prevenir a los usuarios de descarga malware.
3.2.14.4	La solución debe prevenir los ataques de phishing y la reutilización de credenciales corporativas en sitios web diferentes a los de la organización.
3.2.14.5	La solución debe bloquear el acceso a sitios web considerados inapropiados de acuerdo a las políticas de la organización.
3.2.15	**SASE INTERNET ACCESS**
3.2.15.1	La solución debe combinar las protecciones en el dispositivo y en la nube para ofrecer una experiencia de usuario mejorada.
3.2.15.2	La solución debe permitir inspección del tráfico en el dispositivo para reducir la latencia y mejorar la precisión de la localización.
3.2.15.3	La solución debe ofrecer mecanismos de protección en el dispositivo utilizando una combinación de tecnologías de prevención de amenazas para proteger los dispositivos de los usuarios contra una amplia gama de amenazas, incluidas las amenazas de día cero, el phishing y el ransomware.
3.2.15.4	La solución debe incluir un motor de prevención de malware que detecte y bloquee el malware antes de que pueda dañar los dispositivos de los usuarios. El motor de prevención de malware se debe actualizar constantemente con las últimas definiciones de malware. Incluso cuando no se se encuentren conectados a la red corporativa.
3.2.15.4	La solución debe proporciona una protección Wi-Fi integrada que proteja a los usuarios contra

	ataques Wi-Fi. La protección Wi-Fi debe cifra el tráfico Wi-Fi para evitar que los atacantes lo intercepten
3.2.15.5	La solución se debe basar en un concepto de SWG (Secure Web Gateway) híbrido que combine las ventajas del SWG basado en la nube y del SWG local. Debe disponer de un SWG basado en la nube que funciona en conjunto con un agente de SWG basado en el dispositivo
3.2.15.6	La solución debe permitir una configuración flexible de políticas
3.2.15.7	La solución debe permitir realizar comprobaciones de postura del dispositivo para garantizar que solo los dispositivos que cumplan condiciones de seguridad específicas puedan acceder a su red.
3.2.15.8	La solución debe agregar una capa adicional de seguridad al verificar la postura o estado de la conexión segura y verificar el dispositivo que se encuentre limpio de malware antes de que pueda acceder a las aplicaciones internas de la organización.
3.2.16	**SOPORTE**
3.2.16.1	**SOPORTE FABRICANTE:** El fabricante debe brindar un soporte en horario de 24x7 (Las 24 horas del día, los 7 días a la semana) desde la firma del contrato. El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de la vigencia del contrato.
3.2.16.2	**SOPORTE PROVEEDOR:** El proveedor debe brindar un soporte en horario de 24x7 (24 horas del día, los 7 días de la semana) remoto o presencial según lo solicite la entidad a partir de la firma del contrato, en caso de requerir cambios de equipos o partes por el fabricante, el proveedor debe asumir todos los costos por desplazamiento, instalaciones, configuraciones y demás que sean necesarios en sitio y esto no incurrirá en ningún costo para el Ejército Nacional. **Tiempos de respuesta:** El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el supervisor del contrato. Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente. De ser necesario el proveedor deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas. El tiempo máximo permitido para restablecer el servicio es de 4 horas.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

De acuerdo con las especificaciones, todos los equipos suministrados por el proveedor deben estar embalados en las cajas originales de fábrica y deben ser totalmente nuevos, sin uso previo. Esto garantiza que los equipos sean entregados en condiciones óptimas y cumplan con las expectativas de calidad y funcionamiento.

Es responsabilidad del proveedor garantizar, mediante un certificado escrito avalado por el fabricante y/o distribuidor autorizado, que los equipos no tienen ningún tipo de licenciamiento adicional al que se describe en la ficha técnica. En caso de que se requiera un licenciamiento adicional que no esté incluido, el proveedor será responsable de cubrir el costo de dicho licenciamiento adicional, sin que esto genere ningún costo para el Ejército Nacional.

Es importante destacar que los equipos suministrados deben ser completamente nuevos y no re manufacturados. Esto asegura que los equipos sean de última generación y estén en perfectas condiciones.

Cada equipo debe ser entregado con sus respectivas cajas individuales y manuales técnicos, manuales de operación, cargador, interfaces de conexión y software de configuración (drivers) en medios digitales originales. Estos componentes adicionales garantizan que se puedan utilizar y operar adecuadamente. Además, los manuales deben estar disponibles

en idioma inglés y/o español, lo que facilitará el entendimiento y uso de los equipos por parte del personal del Ejército Nacional.

3.3.2 Rotulado.

Los equipos suministrados por el proveedor deben contar con un sticker adhesivo que incluya la siguiente información:

- Nombre de la empresa proveedora de los equipos.
- Número del contrato correspondiente a la adquisición de los equipos.
- Número telefónico de contacto para el soporte técnico.
- Correo electrónico de contacto para el soporte técnico.

Este sticker adhesivo deberá colocarse en un lugar visible de cada equipo, de manera que sea fácilmente identificable y accesible para el personal del Ejército Nacional. Esta información permitirá al personal del Ejército Nacional contactar al proveedor en caso de requerir soporte técnico o asistencia relacionada con los equipos suministrados.

Es importante que el proveedor se asegure de que los stickers adhesivos estén claramente legibles y correctamente colocados en cada equipo, de modo que la información sea fácilmente visible y utilizable.

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 compontes del sistema de la solución a adquirir, se debe efectuar una inspección visual para verificar si cada componente cumple con los requisitos generales y requisitos de empaque y rotulado. Se debe tener presente que por sus características y complejidad serán inspeccionados la totalidad de los componentes que hacen parte del sistema integrado.

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado.

Cada uno de los componentes del sistema integrado, debe cumplir con lo establecido en la presente Especificación Técnica en los numerales 3.2 Requisitos Específicos y 3.3 Requisitos de empaque y rotulado. Cuando no se cumpla el criterio de aceptación se rechazará el componente que no cumpla con los criterios establecidos.

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

4.2.1 Muestreo.

Se requerirá la realización de pruebas de funcionalidad con el objetivo de garantizar que la configuración, integración e instalación de las soluciones sean apropiadas. En caso de que se identifiquen fallas técnicas en alguno de los componentes durante las pruebas, el proveedor deberá tomar las medidas necesarias para solucionarlas sin generar costos adicionales para el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa.

Es responsabilidad del proveedor garantizar que todas las soluciones implementadas funcionen correctamente y cumplan con los requisitos técnicos establecidos en el contrato.

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

Para verificar los requisitos específicos de la presente especificación se debe cumplir con el cien por ciento (100%) de lo establecido en el 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.

Es importante destacar que deben ser proporcionados por el proveedor sin generar costos adicionales para el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad.

El proveedor es responsable de garantizar que los equipos y software funcionen correctamente y cumplan con las especificaciones técnicas establecidas en el contrato.

En caso de que alguno de los equipos presente una falla durante el período de garantía, es responsabilidad del fabricante proporcionar los materiales y/o piezas necesarias para su reparación o reemplazo.

- Estos materiales y/o piezas deben cumplir con las mismas características del equipo original o, en su defecto, ser de características superiores.

- El fabricante debe garantizar que los materiales y/o piezas utilizadas en la reparación o reemplazo sean compatibles y cumplan con los estándares y especificaciones técnicas requeridas. Esto asegura que el equipo vuelva a funcionar correctamente y se mantenga su rendimiento óptimo.

5. MÉTODOS DE ENSAYO

En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, el proveedor deberá brindar el soporte necesario, el cual debe incluir como mínimo:

- Cambio de equipos en caso de fallas: Si se identifica que un equipo específico está defectuoso, el proveedor debe reemplazarlo por uno funcional sin costo adicional para el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad.
- Reemplazo de equipos por otros de iguales o superiores características: Si es necesario reemplazar un equipo, el proveedor debe proporcionar uno con características iguales o superiores para garantizar el correcto funcionamiento del sistema.
- Instalación de software: Si la falla está relacionada con el software, el proveedor debe realizar la instalación o reinstalación del software correspondiente para solucionar el problema.
- Configuraciones, puesta en producción y funcionamiento: El proveedor debe llevar a cabo todas las configuraciones necesarias para poner en producción y asegurar el correcto funcionamiento del sistema después de cualquier reemplazo o reparación realizado.

Es importante destacar que el equipo de reemplazo no puede ser remanufacturado ni reparado, debe ser completamente nuevo. Esto garantiza que el equipo cumpla con los estándares de calidad y funcionalidad requeridos por el Ejército Nacional.

Además, el proveedor debe proporcionar los números de serie de los equipos de reemplazo para que se realicen los cambios pertinentes a nivel administrativo en el Ejército Nacional. Esto asegura un registro preciso de los equipos instalados y facilita la gestión de activos por parte del Ejército Nacional.
En resumen, el proveedor tiene la responsabilidad de reemplazar cualquier equipo defectuoso durante las pruebas o instalación con un equipo nuevo, sin remanufacturar ni reparar, dentro de un plazo máximo de 30 días. Los números de serie de los equipos de reemplazo deben ser proporcionados para fines administrativos.

ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO PARA LA ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA HERRAMIENTA DE SEGURIDAD PERIMETRAL FIREWALL PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA HERRAMIENTA DE SEGURIDAD PERIMETRAL FIREWALL PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL.	
1	**OBLIGACIONES GENERALES DEL CONTRATISTA:**

- **Confidencialidad de la Información**

El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción "acuerdo de confidencialidad".

La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización.

A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento.

Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y la de estos pliegos técnicos, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.

El contratista y los recursos humanos que formaran parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el acuerdo de confidencialidad donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros; así mismo, en caso de un ataque cibernético relacionado con las plataformas de seguridad perimetral firewall o presentarse una situación de cualquier naturaleza que llegue a afectar la infraestructura del Ejército Nacional dentro de los términos del contrato y sea necesario el apoyo de personal del equipo prestador de servicios tenga que apoyar en las instalaciones del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, deberá firmar acta de compromiso de confidencialidad.

- **Propiedad Intelectual**

Todos los estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato serán de propiedad del Ejército Nacional, quien podrá reproducirlos, publicarlos y divulgarlos, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos, en cumplimiento de los términos establecidos en la Ley 23 de 1982, modificada por la Ley 44 de 1993 y la Ley 1915 de 2018.

En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército, será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército.

	El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa y por escrito del Ejército Nacional. Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere. • **<u>Documentación</u>** El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización. Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de las plataformas adquiridas, además se debe especificar: - Los recursos necesarios para la instalación. - Cada uno de los pasos que se deben efectuar. - Los tiempos de ejecución de cada uno de los pasos. - Para el desarrollo de la instalación se deberá presentar un cronograma de tareas después de firmada el acta de inicio del contrato. - Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en cada una de las soluciones. - Informe final donde se describa el total de las soluciones, configuraciones y procesos realizados en la ejecución del contrato Informe de cada visita, documentado los procedimientos realizados. • **<u>Otros</u>** El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información.
2	**<u>El contrato debe ser tratado como un proyecto llave en mano.</u>** Para todos los efectos de funcionalidad e interoperabilidad, el contratista debe instalar, configurar, dar soporte y acompañamiento de las soluciones adquiridas y el software instalado, garantizando al Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad el correcto funcionamiento de acuerdo a las especificaciones técnicas requeridas. ***Nota:*** *"Sera considerado un proyecto llave en mano, aquel que asegure el resultado final de manera satisfactoria, cumpliendo las especificaciones. La optimización de costo, logística, mejores prácticas de implementación serán potestad del contratista, siempre y cuando cumplan con el objetivo final de suministrar una solución que garantice las especificaciones técnicas requeridas; de ser necesario el oferente asumirá costos adicionales de servicios, accesorios, componentes de software, hardware, cableado y elementos adicionales requeridos para la óptima implementación de esta solución e integración con todas las soluciones tecnológicas del Ejercito Nacional."* Se debe suministrar por parte del contratista la logística necesaria para el desarrollo del contrato como: portátiles, desplazamientos, hospedajes, alimentación, discos duros extraíbles, papelería y software para

	el desarrollo del contrato, sin que esto genere costo adicional para el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad; Una vez finalizado el contrato, a estos elementos se les debe realizar un procedimiento de borrado seguro por parte de la Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional para posteriormente ser retirados de las instalaciones del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad.
3	**Cumplimiento de Normatividad Gubernamental en Materia de Tics** Todas las soluciones deben ser compatibles con los protocoles IPV4 e IPV6 CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS Los bienes y servicios TICS contemplados en la presente ficha técnica, deben brindar soporte al protocolo de internet versión seis (IPv6) de conformidad con la Resolución 2710 del 03 de octubre de 2017 de MINTIC, que en su Artículo 5. "Contratación", estipula: "A partir de la entrada en vigencia de la presente resolución, todos los procesos de selección que inicien las entidades públicas deberán, desde los mismos pliegos de condiciones o lo que haga sus veces, exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TICS." **Cumplimiento Normas Técnicas** El Contratista debe cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso: ANSI/TIA-568-C.0 Generic Telecommunications Cablingfor Customer Premises 2009. Norma que dicta las directrices para cableado genérico de telecomunicaciones en instalaciones de clientes. ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard 2009. Norma internacional que estipula las condiciones del cableado de telecomunicaciones para una edificación comercial. ANSI/TIA-568-C.3 Optical Fiber Cabling Components 2000. Norma que crea y estipula directrices generales de los componentes de fibra óptica de un sistema de telecomunicaciones. ANSI/TIA-568-C.2 Commercial Building Telecommunications Cabling Standard Agosto 2009. Norma que crea y estipula directrices de los diferentes componentes de un sistema de telecomunicaciones basado en transmisión en cables de pares trenzados.Telecomunicaciones/Infraestructuras Comerciales). ANSI-J-STD 607 y adendos "Commercial Building Grounding and Bonding Requirements for Telecommunications" (Requisitos para Telecomunicaciones de Puesta y Unido a Tierra en Edificios Comerciales). ANSI/TIA/EIA-526-7 "Measurement of Optical Power Loss of Installed Single-ModeFiber Cable Plant" (Medición de la Pérdida de Potencia Óptica de la Planta Instalada de Cable de Fibra Monomodo). ANSI/TIA/EIA-526-14ª"Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant" (Medición de la Pérdida de Potencia Óptica de la Planta Instalada de Cable de Fibra Multimodo). IEC/TR3 61000-5-2 – Ed. 1.0 y enmiendas "Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 2: Earthing and cabling" (Compatibilidad electromagnética (EMC) – Parte 5: Directrices de instalación y mitigación – Sección 2: Conexión a tierra y cableado). ISO/IEC 11801:2000 Ed2.0 y enmiendas "Information technology – Generic cabling for customer premises" (Cableado Genérico para Propiedades de Usuario). CENELEC EN 50173:2000 y enmiendas

<table>
<tr><td></td><td>ANSI/TIA 942 Telecommunications Infrastructure Standard for Data Centers.

ISO/IEC 24764 draft Generic cabling for Data Centre premises.

Código Eléctrico Nacional NEC /RETIE (NTC 2050 de 1998).

ICONTEC, para la construcción y fabricación de materiales y equipos

NEMA, NEC: En caso de existir vacíos en lo referente a aspectos particulares en las Normas locales.

El Contratista deberá cumplir con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) que se encuentra en la norma NTC 2050.

El contratista deberá contar con el certificado de conformidad de los productos comprendidos en al alcance del RETIE, para los siguientes elementos:

- Tomacorrientes
- Cable Eléctrico
- Tableros
- Tubería

Protecciones (breakers y tomas con supresor de transientes).</td></tr>
<tr><td>4</td><td>El oferente debe incluir en la oferta, un cuadro de marcas y referencias de los equipos a ofertar con su respectivo catalogo o ficha técnica y el detalle técnico.

El oferente debe adjuntar la documentación oficial del fabricante del producto donde se evidencie el cumplimiento de las especificaciones técnicas, la cual debe estar en un sitio web público oficial del producto (fabricante) y/o mediante manuales de configuración y/o descripción del producto en los cuales se pueda evidenciar el cumplimiento de las especificaciones técnicas solicitadas.

Dentro del sitio web y/o documentación oficial debe encontrarse los términos en idioma español (si la documentación oficial es en inglés, el oferente debe adjuntar la traducción al idioma español) que identifique fácilmente el cumplimiento de los requerimientos técnicos solicitados por la entidad, NO se aceptarán cartas firmadas como prueba de validación de especificaciones técnicas ya que deben estar públicos o en documentación oficial de los productos.

<table>
<tr><td>Cantidad</td><td>Elemento</td><td>Marca</td><td>Referencia</td><td>Detalle técnico</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Los equipos deben tener un sticker adhesivo con el nombre de la empresa que suministra los equipos, el número del contrato, número telefónico y correo electrónico donde brindan soporte técnico.

Todos los equipos deberán estar embalados en las cajas de la fábrica y deben ser totalmente nuevos. La instalación de las licencias ya debe venir incluida en cada máquina que a partir de la firma del contrato serán Propiedad del Ejército Nacional, así mismo es responsabilidad del contratista garantizar mediante certificado escrito y avalado por el fabricante y/o distribuidor autorizado que los equipos no cuentan con ningún tipo de licenciamiento adicional al que esta descrito en esta ficha, de no ser así será responsabilidad del contratista el costo del licenciamiento adicional lo que no generara costo alguno para el Ejército Nacional.
De igual modo los equipos deben ser nuevos y no remanufacturados.

Cada uno de los equipos será entregado con sus respectivas cajas individuales y manuales técnicos, manuales de operación, cargador, interfaces de conexión, software de configuración (drivers) en medios digitales originales, para cada uno de los componentes del equipo que garanticen su pleno funcionamiento.</td></tr>
</table>

	Los manuales deben contener idioma ingles y/o español. El contratista deberá adjuntar en archivo digital e impreso en Excel el listado de los seriales, referencias, periodo de garantía, licenciamiento, de todos los equipos a entregar con el fin de verificar de una forma rápida el material. Los equipos deben tener un stickeradhesivo con el nombre de la empresa que suministra los equipos, el número del contrato, número telefónico y correo electrónico donde brindan soporte técnico.
5	El contratista debe garantizar que toda representación gráfica debe cumplir normas fijas y preestablecidas para poder describir de forma exacta y clara; equipos, asignación de recursos físicos y licencias, al igual que dimensiones y características que permitan identificar la plataforma adquirida y habilitar la construcción del nuevo diseño elaborado. Al finalizar la implementación el contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware y Software con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.
	El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, conversores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo al diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de las soluciones, lo cual no incurrirá en costos adicionales para el Ejército Nacional.
6	Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.
7	Para la implementación y conectorización eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato.
8	El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones.
9	**<u>Soporte Fabricante</u>** Según las especificaciones proporcionadas, el horario de cobertura de soporte por parte del fabricante debe ser 24x7x365, lo que significa que debe estar disponible los 365 días del año, las 24 horas del día, incluyendo días festivos. Esto garantiza que el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad pueda recibir asistencia técnica y soporte en cualquier momento, incluso fuera del horario laboral regular. En cuanto a las actualizaciones de software, el fabricante debe proporcionarlas sin costo adicional durante el periodo de vigencia del contrato. Esto garantiza que el software utilizado en la solución se mantenga actualizado y cuente con las últimas mejoras y correcciones de seguridad sin incurrir en costos adicionales. Es importante tener en cuenta que estos aspectos relacionados con el soporte, la cobertura horaria y las actualizaciones de software deben ser detallados y especificados tanto en el contrato como en los términos de garantía, para asegurar que ambas partes, el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberdefensa el contratista, estén de acuerdo y cumplan con estas condiciones durante la ejecución del contrato. El término de la garantía técnica por parte fabricante será de mínimo dos (02) años para cada elemento desde la firma del acta de recibo a satisfacción.

	El Fabricante atreves del contratista debe incluir los servicios de revisión y validación del estado de salud de la plataforma generando informes para optimización y verificación de casos específicos solicitados por el supervisor del contrato.
10	**Soporte Contratista** El contratista debe ofrecer el servicio de soporte técnico de la garantía para los sistemas y/o productos descritos en las Especificaciones Técnicas, durante la ejecución del contrato, es decir por un periodo de 2 años que es el término de la garantía. El horario de soporte por parte del contratista debe ser 24x7x365 remoto o presencial según lo solicite la entidad a partir de la firma del contrato, en caso de requerir cambios de equipos o partes por el fabricante, el contratista debe asumir todos los costos por desplazamiento, instalaciones, configuraciones y demás que sean necesarios en sitio y esto no incurrirá en ningún costo para la entidad. **TIPO DE ATENCIÓN**: El servicio será prestado de dos formas así: • Soporte Nivel 1: De manera presencial tres días a la semana con duración de 8 horas laborales (3x8) en las instalaciones Ejército del Cantón Militar "Caldas" Cra 46 # 20c -01 Bogotá o donde se encuentre el sistema, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato, durante la vigencia de contrato. Para prestar este servicio el ingeniero de soporte debe contactar con equipo de cómputo suministrado por el contratista el cual se dejará en las Instalaciones del Batallón de Ciberdefensa y Seguridad durante la vigencia del contrato. • Soporte Nivel 2: Cuando se requiera remotamente a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato Para este soporte el contratista deberá suministrar un servicio de asistencia técnica con personal certificado para atender necesidades específicas de la plataforma. **Tiempos de respuesta:** El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional durante la duración del periodo de garantía. Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente. De ser necesario el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas. El tiempo máximo permitido para restablecer el servicio es de 4 horas.
11	**Garantía** El Contratista durante los primeros 15 días posteriores a la reunión de inicio deberá indicar el procedimiento que se deberá seguir para solicitar el servicio de garantía, tanto del hardware como de software de los servicios implementados. El término de la garantía técnica por parte fabricante será de mínimo dos (02) años para cada elemento El término de la garantía técnica por parte del contratista será de mínimo dos (02) años para cada elemento desde la firma del acta de recibo a satisfacción. **NOTA:** El Oferente deberá incluir con la oferta el procedimiento que se deberá seguir para solicitar el

	servicio de garantía, tanto del hardware como de software de los servicios implementados.
12	**Certificación de Fabricante** El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado en la herramienta y que está autorizado para distribuir y dar soporte de los productos adquiridos. El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado Check Point Certified Support Provider (CSP/CCSP) y que está autorizado para distribuir con un nivel de experiencia profesional o superior y dar soporte de los productos relacionados en la presente especificación técnica. El oferente deberá presentar carta del fabricante de la solución propuesta la cual avale la solución ofertada para el cumplimiento de todas las características técnicas. El contratista durante los primeros 5 días después de formalizado el contrato se compromete a entregar al supervisor una certificación o documento que soporte la compra de la solución propuesta expedido por el fabricante.
13	**SERVICIO DE MIGRACIÓN E IMPLEMENTACIÓN:**
13.1	**Implementación del Proyecto** El contratista junto con el supervisor debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con la seguridad perimetral. El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones. Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Ejército Nacional. El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Ejército Nacional que sean necesarias para el óptimo funcionamiento de todas las tecnologías. El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware y Software con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional. El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, conversores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo al diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de las soluciones, lo cual no incurrirá en costos adicionales para el Ejército Nacional. Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6. Para la implementación y conectorización eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado

	programado, este debe ser coordinado con el supervisor del contrato.
13.2	**Caso de Fallas** Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. El Contratista en caso de que al momento de las pruebas o instalación de las soluciones si algún equipo sale defectuoso el contratista está en la obligación de reemplazar los equipos por uno de las mismas características y/o superiores en un plazo no mayor a 30 días. El equipo no puede ser remanufacturado o reparado debe ser totalmente nuevo y deberá enviar los números de seriales para realizar los cambios pertinentes administrativos en el Ejército Nacional. En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo: Cambio de equipos en caso de fallas. Remplazo de equipos por otros de iguales o superiores características. Instalación de software. Configuraciones, puesta en producción y funcionamiento En caso de falla de alguno de los equipos, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o reemplazo de características iguales o superiores. En el caso de un reemplazo o adquisición de un nuevo appliance para el arreglo, la solución debe incorporarlo al Clúster en menos de 10 minutos, minimizando la intervención humana dentro del proceso.
13.3	Migración: El contratista deberá realizar una reunión inicial para el levantamiento de información y planificación para la implementación de la solución. El contratista deberá entregar un plan de trabajo y cronograma de trabajo donde se evidencien los recursos, tiempos, requisitos, factores críticos de éxito y responsables del proceso de implementación El contratista aplicara las mejoras prácticas de seguridad y ajustarlas a las políticas de seguridad informática de seguridad informática del Ejército Nacional. El contratista deberá integrar los equipos a la red y configurará el enrutamiento y la dirección IP. El contratista deberá contemplar dentro de su oferta todo el costo asociado al cableado estructurado, patch cord de cobre, fibra ópticas y demás elementos que se requiera para la implementación y puesta en funcionamientos de la solución la integración con Dos y el SW CORE que cuenta el Ejército Nacional Integración: Realizar una correcta instalación: Es importante realizar una correcta instalación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware y software. Configuración adecuada: La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red.

	Pruebas de integración: El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.
14	**TRANSFERENCIA DE CONOCIMIENTO**
14.1	El Contratista debe realizar transferencia de conocimiento para 02 personas, del Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional curso CCSE, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica.
15	**RECURSOS HUMANOS**
15.1	• Implementación: La implementación debe ser realizada por el contratista de acuerdo a los siguientes perfiles, de la cual el oferente deberá presentar junto con la oferta los siguientes requerimientos: Líder o gerente del Proyecto: Profesional responsable de coordinar y supervisar la ejecución del contrato, así como de comunicarse con el supervisor del contrato para garantizar el cumplimiento de los objetivos y las obligaciones establecidas, encargado de la implementación de la tecnología a adquirir y con quien se gestionarán el cumplimiento del objeto del contrato, debe cumplir con los siguientes requisitos. ✓ Se requiere que el rol del líder o gerente del proyecto, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a cuatro (04) años. ✓ Debe haber sido líder técnico de proyectos de seguridad. ✓ Debe acreditar al menos tres (3) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de la solución adquirir ✓ Certificación o constancia de temas de ciberseguridad en la solución ofertada emitido por el fabricante. Implementación: Profesional operativo que se encargará de la implementación y despliegue de la solución a adquirir, generación de reglas y políticas, configuración de reglas y generación de estándares para la clasificación sensible de activos de información, aplicación de buenas prácticas de seguridad. ✓ Se requiere que la implementación de la solución, la realice como mínimo uno (01) ingenieros con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a cuatro (03) años con especialización en seguridad informática. ✓ Debe acreditar al menos tres (3) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de redes o seguridad de informática o implementación de la solución. ✓ Deberá contar con las siguientes certificaciones: o Debe contar con la certificación nivel experto CCSE y CCTE (vigentes a la fecha de cierre del proyecto) o Debe haber participado en mínimo un proyecto de implementación o soporte de firewalls virtuales o Certificación CCNP. o Certificación o constancia de entrenamiento en la solución ofertada emitido por el fabricante o por un ente certificador autorizado por el fabricante. Soporte: Profesional operativo que se encargará posterior a la implantación, de las labores de mantenimiento de la solución instalada, garantizando el correcto funcionamiento y velando por que las políticas y configuraciones de acuerdo a requerimientos del Supervisor, durante la vigencia de ejecución del contrato hasta el término de la garantía, y de acuerdo con los términos y tiempos de respuesta

especificados en el ítem 3.2.16.2 en el documento de Especificaciones técnicas.

- ✓ Se requiere que el ingeniero soporte de la solución, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a dos (02) años.
- ✓ Debe adjuntar certificación CCSE (Check Point Certified Security Expert) y certificación CCSA (Check Point Security Administrator y/o CCTE (Check Point Certified Troubleshooting Expert y/o CCSM (Check Point Certified Security Masters).
- ✓ Debe acreditar al menos dos (2) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de soluciones de redes o seguridad de informática o implementación de seguridad perimetral.

ALCANCE SOPORTE

Se debe desarrollar como mínimo las siguientes actividades durante la vigencia del contrato preveía autorización y aprobación del supervisor del contrato:

- Administración de plataformas de seguridad perimetral firewalls: responsable de las tareas de comprobación de funcionamiento, administración, gestión, control y aplicación de las plataformas de seguridad perimetral firewall.
- Generar recomendaciones para las buenas prácticas de administración de políticas en las plataformas de seguridad perimetral firewall.
- Monitorizar el funcionamiento de la plataforma de seguridad perimetral firewalls.
- Revisión, control y mantenimiento de la estabilidad y operación de las plataformas de seguridad informática descritas.
- Generar recomendaciones para la actualización de las plataformas de seguridad perimetral firewalls del Ejercito Nacional.
- Configuración de políticas, realizar evaluación y ajuste de la configuración de las políticas de seguridad implantadas en todas las plataformas de seguridad perimetral firewalls, bajo la supervisión del administrador de Seguridad del Ejército Nacional.
- Atención a solicitudes: Para ello evaluará y ejecutará nuevos requerimientos de configuración sobre las plataformas de seguridad perimetral firewalls.
- Seguimiento de backups: Gestionar y efectuar las copias de resguardo (back-up) de la información de las herramientas de seguridad del sistema y de completar la documentación correspondiente a esta tarea.
- Integración del Directorio Activo con las plataformas de Seguridad Perimetral Firewalls del Ejercito Nacional.
- Revisión y seguimiento de políticas de passwords: El administrador de seguridad deberá realizar periódicamente un seguimiento de la implementación de las políticas de passwords, con el propósito de verificar que las mismas se encuentran en fase con lo definido.
- Seguimiento de la actualización de herramientas de seguridad: el administrador de seguridad será el responsable de verificar que las herramientas de seguridad descritas en este documento, se encuentren en regla y actualizados con los correspondientes soportes y mantenimientos ejecutados por el proveedor del contrato de soporte y mantenimiento.
- Afinamiento a la infraestructura de seguridad perimetral Firewalls actual.
- Nuevas configuraciones o activaciones de nuevas funcionalidades del producto, previa coordinación con el personal técnico y el supervisor del contrato.
- Pruebas de puesta en funcionamiento de nuevos servicios de seguridad perimetral firewall.
- Realizar levantamiento de la topología de red de la infraestructura de seguridad perimetral Firewalls del Ejército Nacional.
- Sugerir recomendaciones en coordinación con la administración de seguridad perimetral y el supervisor del contrato para implementar nuevas políticas de firewalls, mejoramiento IPS y control de aplicaciones.

	• Atención ilimitada a casos reportados por el Batallón de Ciberdefensa y Ciberseguridad (BACCI) del Ejército Nacional referentes a cualquier evento relacionado con el funcionamiento, administración e incidentes o eventos de seguridad de la plataforma de seguridad informática. **ALCANCE MANTENIMIENTO PREVENTIVO:** El contratista debe efectuar dos (02) mantenimiento preventivo durante la ejecución del contrato según cronograma acordado entre el contratista y el supervisor del contrato a las plataformas de seguridad perimetral Firewalls del Ejército Nacional. Este mantenimiento debe incluir como mínimo las siguientes actividades: • Actualizaciones de software (Upgrade, Update, criticas de seguridad) • Revisiones del funcionamiento de las plataformas y solución de errores. • Realización y programación de copias de seguridad. • Revisión de los logs de eventos registrados en los sistemas. • Revisión y mejoramiento de espacio de disco, utilización de CPU – RAM y afinamiento de servidores. • Evaluación de los sistemas de seguridad instalados. • Configuración de funcionalidades inoperativas. • Emisión de recomendaciones de las plataformas a través de un informe técnico, al supervisor del contrato. • El contratista deberá suministrar el recurso en sitio donde se requiera realizar este mantenimiento se podrán realizar de manera remota, pero si algo falla y no se puede subsanar el contratista desplazará al personal especializado hasta el sitio. **ALCANCE MANTENIMIENTO CORRECTIVO:** En caso de presentarse fallas en los sistemas de seguridad perimetral firewall del Ejercito Nacional, el contratista deberá efectuar los mantenimientos correctivos todas las veces que se requiera. Estos mantenimientos deben incluir como mínimo: • Instalación de software • Configuraciones, puesta en producción y funcionamiento • Remplazo de equipos por otro de iguales características de forma temporal hasta que la falla sea solucionada. **Nota1:** Los ingenieros deben ser de nacionalidad colombiana **Nota2:** El oferente deberá presentar junto con la oferta las hojas de vida con sus respectivas certificaciones académicas y de experiencia laboral en las funciones requeridas para los anteriores perfiles: <u>Para realizar la validación correspondiente del personal requerido, el oferente debe aportar la siguiente documentación del personal encargado de estas actividades.</u> Copia legible del diploma de pregrado como ingeniero de sistemas, o electrónico, o de telemática, o comunicaciones y/o afines conforme al SNIES a estas profesiones. • Copia legible de la tarjeta profesional • Copia de cédula de ciudadanía que verifique la nacionalidad colombiana. • Carta de compromiso de participación del personal firmada por la profesional dirigida al proceso. • La experiencia se deberá certificar considerando los siguientes aspectos que se relacionan a continuación: ▪ Nombre o razón social del contratante ▪ Descripción de las actividades realizadas ▪ Fecha de iniciación del contrato

	▪ Fecha de terminación del contrato ▪ Dirección y teléfono de quién expide la certificación Otras obligaciones del contratista: El Contratista, durante la ejecución del contrato, acepta que el Ejército Nacional evalúe el desempeño profesional de la(s) persona(s) asignadas para el proyecto y estará(n) en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del supervisor del contrato. Durante la ejecución del contrato, si se requiere reemplazar un funcionario por otro, éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado, y cumplir con los requerimientos estipulados en esta especificación técnica. En caso de que el contratista requiera realizar un cambio de personal, este deberá informar al supervisor del contrato de tal situación con mínimo 10 días de antelación, anexando la hoja de vida del nuevo funcionario que debe cumplir con las especiaciones requeridas. El supervisor evaluará el desempeño laboral del profesional asignado para el soporte y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.

Cordialmente,

(Firma – posfirma representante legal o apoderado)
Proponente:
Documento de Identidad: