ANEXO ESPECIFICACIONES TECNICAS 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 la Invitación a ofertar, ofertó de forma irrevocable, los siguientes bienes o servicios objeto del presente proceso de contratación, con las siguientes características técnicas:

Para efectos de establecer las especificaciones técnicas del presente proceso, se dará aplicación a la FICHA TECNICA **"HERRAMIENTA PARA LA MIGRACION DE ATAQUES DE DDoS EL FORTALECIMIENTO DE LOS MEDIOS CEBERNETICOS DEL EJERCITO NACIONAL No. JEMPP-CEDE6-BACCI-ET-04070/ COMUN-01**, el cual contiene los parámetros técnicos que deben cumplir los oferentes en la acreditación de los servicios a prestar, así mismo, el contenido es el mismo del **ANEXO ESPECIFICACIONES TÉCNICAS**.

3.2 REQUISITOS ESPECIFICOS

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 que brindan protección ante intrusos y denegación de servicios 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.

3.1.1	**REQUERIMIENTO GENERAL:**
3.1.1.1	El contratista deberá proveer, instalar, configurar y poner en funcionamiento, un equipo de comunicación y seguridad tipo Appliance para realizar la protección contra denegaciones de servicio, que proporcione las siguientes funcionalidades: ● Mitigación de ataques de DDoS utilizando análisis de comportamiento. ● Afinamiento de las líneas base y firmas en tiempo real. ● Mitigación de ataques basados en anomalías, escaneos, paquetes fuera de estado. ● Módulo de IPS. ● Etapas de aprendizaje de las políticas y afinamiento de las configuraciones para ser puestas en modo bloqueo.

3.2. Requisitos específicos

ÍTEM	**Requisitos**
3.2.1	**ARQUITECTURA**
3.2.1.1	La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.
3.2.1.2	Debe soportar despliegues fuera de línea usando puertos SPAN o puertos mirror.
3.2.1.3	La solución de mitigación de ataques DDoS debe tener la siguiente configuración de interfaces para su integración a la red. • 12 Interfaces SFP+ de 10 GE. Incluír tranceivers para la protección de 2 de enlaces de 10GE con fibra multimodo y 1 un enlace de 1GE en cobre. ● - 6 Interfaces QSFP+ de 40 GE.
3.2.1.4	La solución debe contar con un bypass de hardware, que garantice la disponibilidad de la conectividad en caso de falla de hardware.
3.2.1.5	La solución debe soportar bypass por software para pares de puertos individuales.

3.2.1.6	La solución de mitigación de ataques DDoS debe soportar la inspeccion de los encabezados internos o externos de tuneles L2TP, GRE, GTP, IPinIP.
3.2.1.7	La solución debe poder monitorear y alertar sobre el uso de CPU de cada politica definida de forma independiente.
3.2.1.8	La solución de mitigación de ataques DDoS debe soportar IPv4 e IPv6.
3.2.1.9	La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.
3.2.1.10	La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable
3.2.1.11	Debe permitir la segregación por usuario o por grupo de usuario, por política de protección, limitando el acceso de los usuarios o grupos solamente a las políticas asignadas.
3.2.2	**CAPACIDAD**
3.2.2.1	La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 20 Gbps por equipo.
3.2.2.2	La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 40 Gbps por equipo
3.2.2.3	La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 40 Gbps por equipo.
3.2.2.4	La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 30 Millones PPS (paquetes por segundo) por cada equipo adquirir.
3.2.2.5	La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos.
3.2.2.6	La solución de mitigación de ataques DDoS debe incluir hardware dedicado para la mitigación de ataques SSL / TLS con capacidad de al menos 90.000 CPS con llaves RSA de 2K y debe soportar TLS 1.3 en hardware.
3.2.3	**FUNCIONALIDADES DE DETECCIÓN Y MITIGACIÓN DE ATAQUES**
3.2.3.1	La solución debe proteger contra al menos las siguientes anomalías de tráfico: ● Checksum incorrecto de IPV4. ● Encabezado IPv4 o Longitud total invalido. ● Tamaño de Cabecera capa 4 invalido. ● TTL igual a 0. ● Cabecera IPV6 inconsistente. ● Límites de salto IPV6 alcanzados. ● Protocolo Capa 4 no soportado. ● TCP flags invalido. ● Tamaño de cabecera UDP 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.
3.2.3.2	La solución debe operar a través de políticas de seguridad con distintas configuraciones de detección y mitigación de acuerdo a los objetos protegidos.
3.2.3.3	Las políticas de seguridad se podrán habilitar o deshabilitar individualmente.
3.2.3.4	Las políticas de seguridad se podrán configurar en modo reporte o en modo bloqueo.
3.2.3.5	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.

3.2.3.6	La solución debe contar con análisis de comportamiento de red para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo como mínimo las siguientes inundaciones de tráfico: ● Inundación de red UDP. ● Inundación de red ICMP. ● Inundación de red IGMP. ● Inundación de red TCP con flag SYN. ● Inundación de red TCP con flag RST. ● Inundación de red TCP con flag PSH. ● Inundación de red TCP con flag FIN. y ACK. ● Inundación de red TCP con flag SYN y ACK. ● Inundación de red TCP flag FRAG. ● Inundación de red UDP con flag FRAG.
3.2.3.7	La solución debe incluir un mecanismo preciso de detección de inundaciones UDP que tenga en cuenta parámetros que varíen con la tasa de tráfico y parámetros que no varíen con la tasa de tráfico, incluyendo: ● Ancho de banda UDP. ● Tasa de paquetes por segundo. ● Tasa de conexiones por segundo.
3.2.3.8	La solución debe permitir configurar un umbral de ancho de banda de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.
3.2.3.9	La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener los ataques en capa de red.
3.2.3.10	La solución debe proteger contra ataques de tipo ráfaga (burst attacks) identificando que una nueva ráfaga de tráfico pertenece a una firma en tiempo real previamente creada.
3.2.3.11	La solución debe incluir un mecanismo de prevención de overblocking de tráfico el cual valide y refresque la firma, si se está bloqueando más tráfico del debido.
3.2.3.12	La solución debe permitir especificar un límite de tasa de tráfico que servirá como un método alternativo automático a la firma en tiempo real de red.
3.2.3.13	La solución de mitigación de ataques DDoS debe incluir un mecanismo de límite de conexiones TCP y sesiones UDP que cumpla con las siguientes características: ● La solución debe contar el número de conexiones TCP o sesiones UDP abiertas por cliente, por servidor, o por la combinación de cliente y servidor. ● La solución debe permitir descartar los paquetes que pasen el límite establecido. ● La solución debe permitir suspender el tráfico por un tiempo determinado si este pasa del límite establecido.
3.2.3.14	La solución de mitigación de ataques debe incluir un mecanismo que haga seguimiento y bloquee paquetes que superen una tasa de PPS en sesiones definidas.
3.2.3.15	La solución debe incluir protección contra ataques DDoS de inundación de paquetes fuera de estado.
3.2.3.16	La solución debe incluir protección contra ataques DDoS de tipo SYN Flood
3.2.3.17	La protección contra ataques SYN Flood a través del seguimientos de paquetes SYN enviados a cada IP destino y puerto.
3.2.3.18	La protección de SYN Flood debe prevenir contra ataques de tipo Spoofed-SYN-flood que vayan dirigidos a múltiples puertos destinos, a través del seguimiento de paquetes SYN enviados a toda la red configurada en la política.
3.2.3.19	La protección de SYN Flood debe contar con al menos dos métodos de autenticación TCP: ACK fuera de secuencia y proxy transparente.
3.2.3.20	La protección de SYN Flood, para http, y https debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script.

3.2.3.21	La autenticación de https debe contar con un mecanismo que permita hacer seguimiento a las IP orígenes y enviar la autenticación solo a aquellas IP que se consideren sospechosas.
3.2.3.22	Los filtros de tráfico deben permitir como mínimo seleccionar los siguientes criterios para hacer match al tráfico: ● Red de Origen. ● Red de Destino. ● Puerto Origen. ● Puerto Destino. ● Protocolo. ● Tamaño del Paquete. ● Flags TCP. ● Time to Live (TTL). ● Número de Secuencia TCP. ● Type of Service (ToS) / DSCP. ● Fragment Offset. ● Fragment ID.
3.2.3.23	Los filtros de tráfico deben permitir configurar límites de tráfico en PPS o bps, sobre el tráfico que haga match con los criterios definidos.
3.2.3.24	La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, MX, PTR, TEST, SOA, NAPTR, SRV, otros.
3.2.3.25	La solución debe aprender acerca del tráfico DNS y configurar automáticamente las líneas bases de tráfico y thresholds ataques por cada tipo de query de forma independiente.
3.2.3.26	La solución debe permitir configurar un umbral de QPS de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.
3.2.3.27	La solución debe crear de forma automática una lista de subdominios permitidos para bloquear ataques de inundación de DNS recursivos (inundaciones de subdominios aleatorios)
3.2.3.28	La solución debe permitir que se cargue un listado con los subdominios permitidos para bloquear ataques de water torture.
3.2.3.29	La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener el ataque de DNS.
3.2.3.30	En condición de ataque DDoS, la solución debe bloquear todo el tráfico hacia el DNS que este fuera del cumplimiento del protocolo DNS.
3.2.3.31	La solución debe incluir un mecanismo de reto y respuesta en DNS para minimizar falsos positivos.
3.2.3.32	La protección de ataques DDoS DNS de la solución propuesta debe basarse únicamente en el tráfico entrante (Ingress-Only o Inbound).
3.2.3.33	La protección de ataques DDoS DNS debe mitigar ataques de tipo fuerza bruta de DNS.
3.2.3.34	La solución de mitigación de ataques DDoS debe proteger contra ataques HTTPS Floods.
3.2.3.35	La protección contra ataques HTTPS debe soportar las siguientes versiones del protocolo SSL usando hardware dedicado: SSL 3.0, TLS1.0, TLS 1.1, TLS 1.2 y TLS 1.3
3.2.3.36	La protección contra ataques HTTPS Flood debe generar baselines y aprender las características del tráfico HTTPS para cada uno de los servidores protegidos.
3.2.3.37	La protección contra ataques HTTPS Flood debe detectar aumentos en las solicitudes HTTPS que no sean parte del tráfico legítimo, con el fin de evitar que un aumento de tráfico legítimo sea catalogada como un ataque.
3.2.3.38	La solución debe ser capaz de detectar y mitigar ataques en HTTPS sin necesidad de descifrar el tráfico previamente.

3.2.3.39	La protección contra ataques HTTPS Flood debe funcionar solo con el tráfico de entrante (Ingress-Only o Inbound).
3.2.3.40	La protección contra ataques HTTPS flood debe identificar automaticamente una lista de IP origen sospechosas del ataque.
3.2.3.41	La protección contra ataques HTTPS Flood podrá anidar distintos métodos de mitigación y dichos métodos escalarán automáticamente en caso de que el ataque no este siendo mitigado.
3.2.3.42	La protección contra ataques HTTPS Flood debe contar con al menos los siguientes métodos de mitigación: - Mitigación del primer request de los fuentes/origenes sospechosos haciendo autenticación HTTPS únicamente a las fuentes/origenes sospechosos. - Limitar la tasa de tráfico a los origenes sospechosos. - Mitigación del primer request de todos las fuentes/origenes haciendo autenticación HTTPS a todos los origenes que se conecten a los servidores protegidos. - Inspección selectiva completa por cada objeto (servidor) protegido, de tal forma que el trafico desencriptado despues sea inspeccionado por firmas en tiempo real en capa 7, filtros de tráfico manuales y firmas de ataques conocidos.
3.2.3.43	La protección contra ataques HTTPS Flood debe contar con un mecanismo de protección contra ataques de tipo low and slow en HTTPS, el cual haga seguimiento a las sesiones concurrentes establecidas por un origen y luego de alcanzar un threshold configurado, realice una auntenticación sobre HTTPS y suspenda aquellos origenes que no puedan ser autenticados.
3.2.3.44	La solución de mitigación de ataques DDoS debe soportar protección Quantile DoS (QDoS) contra micro-inundaciones y pequeños ataques de inundación DoS/DDoS (Phantom floods)
3.2.3.45	La protección Quantile DoS debe soportar los siguientes metodos de mitigación, y deben permitir implementarse de manera escalonada: - Firma en tiempo real generada automáticamente - Top Talkers - Rate Limit
3.2.3.46	Dentro de la protección de Quantile DoS, cada cuantil será independiente, permitiendo detectar y mitigar ataques sobre cada uno de ellos de manera autónoma
3.2.3.47	La protección Quantile DoS debe permitir definir los siguientes niveles de sensibilidad de detección: - 0.5% - 1% - 2% - 5% - 10%
3.2.3.48	La protección Quantile DoS debe permitir definir el máximo ancho de banda permitido por cuantil durante un ataque, el cual será usando por el método de mitigación de rate-limit. - Rate limit Estricto (100% del BW del cuantil) - Rate limit Moderado (150% del BW del cuantil) - Rate limit Permisivo (200% del BW del cuantil)
3.2.3.49	La solución debe permitir crear reglas de listas negras y listas blancas, incluyendo al menos los siguientes parámetros de clasificación: - Red Origen - Puerto Origen - Red Destino - Puerto Destino - Protocolo

3.2.3.50	La solución de mitigación de ataques DDoS debe incluir un mecanismo de protección contra escaneos de puertos TCP, UDP e ICMP
3.2.3.51	La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado.
3.2.3.52	La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado.
3.2.3.53	La solución de mitigación de ataques DDoS debe incluir una protección basada en firmas de ataques conocidos que permita al menos mitigar los siguientes tipos de ataques: -Inundaciones TCP, UDP e ICMP lanzados desde herramientas conocidas. -Vulnerabilidades a nivel de servidores: Web, e-mail, FTP, SQL, DNS, SIP.
3.2.3.54	La protección basada en firmas de ataques conocidos debe incluir grupos de firmas preconfigurados para ser aplicados en las políticas.
3.2.3.55	La protección basada en firmas de ataques conocidos debe permitir crear grupos de firmas por elementos comunes y aplicar los grupos de firmas en las políticas.
3.2.3.56	La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas.
3.2.3.57	La protección basada en firmas debe permitir a los operados crear sus propias firmas.
3.2.3.58	La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas.
3.2.3.59	La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización
3.2.3.60	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 periódicamente.
3.2.3.61	La protección de geolocalización debe permitir la configuración de un perfil y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas. Dentro de dicho perfile se podrán definir al menos las siguientes acciones: - Bloquear las geografías seleccionadas. - Permitir las geográficas seleccionadas.
3.2.3.62	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 periódicamente.
3.2.3.63	La lista de IP debe incluir al menos las siguientes categorías: -Atacantes Activos: Direcciones IP que han sido correlacionados y se han determinado como maliciosas. -Tor Exit Nodes: Una IP que es un Tor Exit Node, sin importar si ha participado o no en actividades de ataques. -Web Attackes: Una IP que ha hecho intentos de violacionaes Web. - Scanners
3.2.3.64	La lista de IP maliciosas, en conjunto con las acciones configuradas por categorías, debe aplicarse sobre cada política de seguridad.
3.2.4	**CONSOLA DE GESTIÓN, MONITOREO Y REPORTERÍA CENTRALIZADA**
3.2.4.1	La consola de gestión debe ser del tipo Virtual Appliance y deberá poder instalarse sobre Hyper-V o Vmware ESXI 5 o superior.
3.2.4.2	La solución debe incluir un elemento de gestión y control centralizado y que soporte la administración y monitoreo de todos los mitigadores que hacen parte de la propuesta.
3.2.4.3	El elemento de gestión y control centralizado debe incluir un panel que permita el monitoreo de toda la solución en tiempo real.
3.2.4.4	La consola de gestión debe soportar la administración y monitoreo del mitigador ofertado.
3.2.4.5	La consola de gestión permitirá asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.

3.2.4.6	La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.
3.2.4.7	El panel de monitoreo en tiempo real debe mostrar el estado general de la solución: - Situación general, si estamos o no bajo ataque. - Resumen de tráfico actual, incluyendo tráfico de descartado y tráfico autenticado.
3.2.4.8	El panel de monitoreo en tiempo real debe incluir un campo de busqueda que permita filtrar la información desplegada utilizando al menos los siguientes criterios: - Filtro a través de una IP específica. - Filtro por el mitigador. - Filtro por política.
3.2.4.9	La consola de gestión debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.
3.2.4.10	La consola de gestión debe permitir la configuración de NTP.
3.2.4.11	El panel de monitoreo en tiempo real debe mostrar un listado de todas las políticas que incluya el estado de cada uno de ellas, indicando al menos: - Si la política se encuentra bajo ataque. - Nombre de la política. - Ancho de banda entrante hacia la política. - Tráfico siendo descartado sobre la política. - Tráfico siendo autenticación.
3.2.4.12	La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.
3.2.5.13	El panel de monitoreo en tiempo real debe mostrar un listado de todas las políticas que incluya el estado de cada uno de ellas, indicando al menos: - Si la política se encuentra bajo ataque. - Nombre de la política. - Ancho de banda entrante hacia la política. - Tráfico siendo descartado sobre la política. - Tráfico siendo autenticación.
3.2.4.14	La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos.
3.2.4.15	La consola de gestión debe permitir sincronización con un servidor NTP.
3.2.4.16	El panel de monitoreo en tiempo real debe mostrar un listado de todos los mitigadores, agrupando las métricas de ancho de banda, tráfico descartado y autenticado u número de políticas por cada mitigador.
3.2.4.17	La consola de gestión debe permitir visualizar la utilización de CPU de los dispositivos administrados.
3.2.4.18	La consola de gestión debe contar con una funcionalidad que permita la captura de paquetes que ingresan y salen del equipo. Estos archivos deberán estar en formato CAP y deben poder descargarse.
3.2.4.19	La consola de gestión debe permitir definir al menos los siguientes parámetros dentro de la captura: Duración, número de paquetes a Capturar, IP origen, IP Destino, Protocolo.
3.2.4.20	La consola de gestión debe permitir creación de tareas calendarizadas de backup de los dispositivos administrados.
3.2.4.21	El panel de monitoreo en tiempo real debe mostrar un listado con los eventos de detección de ataques asociados a las políticas, tanto los que ocurren en tiempo real, como los históricos, aquellos que han ocurrido previamente.
3.2.4.22	La consola de gestión permitirá guardar los backups localmente o enviarlos a un repositorio externo a través de SCP, SFTP o SSH.

3.2.4.23	El listado de los eventos de detección se debe indicar el mitigador, la política de seguridad, nombre del evento, la acción tomada por el mitigador, la categoría del ataque, la duración y la hora de inicio del ataque.
3.2.4.24	Para los ataques detectados la solución debe mostrar el detalle de los mismos incluyendo permitiendo ver muestras de los paquetes que hacen parte del ataque y también descargar PCAPs de los ataques en caso de que aplique.
3.2.4.25	La solución debe permitir realizar capturas en tiempo real con el fin de obtener visibilidad del tráfico tanto en tiempo de paz como durante un ataque.
3.2.4.26	La solución debe incluir un panel de analítica de red que permita el monitoreo de tráfico en tiempo de paz, permitiendo filtras el tráfico por mitigador o por política.
3.2.4.27	La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo.
3.2.4.28	Desde la consola de gestión se podrá realizar la actualización de la versión principal de los dispositivos administrados.
3.2.4.29	Desde la consola de gestión se podrán administrar distintas versiones del dispositivos, teniendo la chance de un rollback de versión en case de necesitarse.
3.2.4.30	La consola de gestión debe permitir la administración de múltiples dispositivos, pudiendo realizar configuración simultánea en varios dispositivos.
3.2.4.31	La consola de gestión debe permitir la creación de scripts y flujos de trabajo para automatizar tareas de configuración recurrentes
3.2.4.32	La consola de gestión debe permitir la comparación de la configuración entre dos dispositivos.
3.2.4.33	La consola de gestión debe permitir la comparación de la configuración entre un dispositivo y un backup determinado.
3.2.4.34	La análitica de red debe incluir como mínimo la siguiente información para cada activo protegido. - Gráficos de Tráfico. - TOP IP Origen. - TOP IP Destino. - TOP Aplicaciones. - TOP Protocolos. - TOP Países - Tendencias de la última semana.
3.2.4.35	La solución de gestión centralizada debe incluir un módulo capaz de realizar reportes con al menos las siguientes caracteristicas: - Capacidad de generar reportes por dispositivo y política de seguridad. - Programar los reportes y enviarlos vía correo electrónico. - Los reportes deben estar disponibles en formatos PDF, HTML o CSV.
3.2.4.36	Los reportes deben ser personalizables y deben permitir elegir la información a incluir en los reportes entre al menos las siguiente información: - Ataques recibidos en el periodo de tiempo seleccionado. - Top ataques por geolocalización. - Gráficos de tráfico (bps y pps), Conexiones por Segundo y Conexiones concurrentes. - TOP Ataques por duración. - TOP Ataques por volumen. - TOP Ataques por acción del mitigador. - TOP Ataques por categoría de amenaza. - TOP IP Destinos atacados. - TOP IP Orignes que atacan. - Ataques por política.

	- Ataques por Firma de seguridad.
3.2.4.37	El módulo de reportes debe incluir un reporte de los ataques generados por la lista de IPs de mala reputación, presentando al menos: - TOP de los ataques por geolocalización. - TOP de los ataques por IP - TOP de los ataques por actividad maliciosa. - Total hits recibidos desde las IP maliciosas
3.2.4.38	La solución debe permitir extraer reportes forenses para analizar ataques, los métodos y tendencias.
3.2.4.39	La solución debe permitir escoger los criterios para generar el reporte forense, con al menos: - Categoría de la amenaza - Nombre del ataque. - Tasa del ataque en bps y pps. - IP Origen / IP Destino. - Duración del Ataque.
3.2.4.40	La solución debe incluir un módulo de alertas que permita definir el impacto y severidad de cada alerta creada y que permita enviarlas via e-mail.
3.2.4.41	El alcance de las alertas generadas debe ser por políticas, permitiendo configurar una o varías políticas por alerta.
3.2.4.42	La solución debe permitir escoger los criterios para generar el reporte forense, con al menos: - Categoría de la amenaza - Nombre del ataque. - Tasa del ataque en bps y pps. - IP Origen / IP Destino. - Duración del Ataque. - Riesgo
3.2.4.43	La consola de gestión debe mostrar en tiempo real los eventos de seguridad detectados por la solución de mitigación de ataques DDoS.
3.2.4.44	El monitoreo en tiempo real de los ataques debe mostrar el estado actual de la infraestructura indicando claramente si hay o no un ataque en curso.
3.2.4.45	El monitoreo en tiempo real debe mostrar estadísticas gráficas del tráfico total entrante y saliente en bits por segundo y paquetes por segundo.
3.2.4.46	El monitoreo en tiempo real debe mostrar estadísticas gráficas de las conexiones por segundo y conexiones concurrentes recibidas.
3.2.5	**LICENCIAMIENTO**
3.2.5.1	El software de la solución debe ser entregado bajo licenciamiento corporativo.
3.2.6	**SOPORTE**

3.2.6.1	**SOPORTE FABRICANTE:** Según las especificaciones proporcionadas, el horario de cobertura de soporte por parte del fabricante debe ser 24x7x365, lo que significa que debe estar disponible los 365 días del año, las 24 horas del día, incluyendo días festivos. Esto garantiza que el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad pueda recibir asistencia técnica y soporte en cualquier momento, incluso fuera del horario laboral regular. 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 un (01) 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.
3.2.6.2	**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 un (01) año 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.

Nota: las especificaciones técnicas HERRAMIENTA PARA LA MIGRACION DE ATAQUES DE DDoS EL FORTALECIMIENTO DE LOS MEDIOS CEBERNETICOS DEL EJERCITO NACIONAL No. JEMPP-CEDE6-BACCI-ET-04070/ COMUN-01, No. JEMPP-CEDE6-BACCI-ET-04070/ COMUN-01,, 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 se encuentra firmado

Elaboró	Revisó	Aprobó
PD06. JOSE EDINSON ROJAS CALDON Profesional Defensa BACCI	M.V. [illegible] GAHENA VASQUEZ Ejecutivo y Segundo Comandante BACCI DR. GLORIA CECILIA CORREA Asesora Jurídica CEDE6	TC. RAMIRO ESTEBAN SILVA GUTIERREZ Comandante del BACCI

ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO PARA ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA HERRAMIENTA PARA LA MITIGACIÓN DE ATAQUES DE DDoS PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL.

	ADQUISICIÓN DE UNA HERRAMIENTA PARA LA MITIGACIÓN DE ATAQUES DE DDoS PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS 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.

- **Documentación**

El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización.

Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de 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 - Entrega de topología 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	**<u>Cumplimiento de Normatividad Gubernamental en Materia de Tics</u>** 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

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.

<table>
<tr><td></td><td>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. 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,</td></tr>
</table>

	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.
6	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.
7	Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.
8	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.
9	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.
10	**<u>Término de Respuesta de la Garantía Técnica</u>** Para el presente proceso de selección, el proponente junto con la oferta deberá presentar el termino de respuesta de la garantía técnica, el cual cubrirá lo siguiente: o El Contratista deberá garantizar el normal funcionamiento de la solución después del funcionamiento y puesta en marcha de la solución, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. o Soporte disponible los 365 días del año en horario 7x24 (7 días a la semana las 24 horas del día) o El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica gratuita, servicio de correo electrónico o en forma remota de acuerdo a los niveles de servicio. En un lapso de cuatro (04) horas después de haber reportado el incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas.

	○ Estarán a cargo del contratista todos los costos en que deba incurrir en el cumplimiento de su deber de garantía. NOTA: Los términos de garantía técnica y el tiempo de respuesta de esta, deberán ser aportados en documento independiente debidamente suscrito por el oferente.
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 un (01) año para cada elemento El término de la garantía técnica por parte del contratista será de mínimo un (01) año 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 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 caso de presentarse fallas ocasionadas por las actividades efectuadas como producto de la ejecución del contrato por parte del contratista, este debe garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados.
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 DDos 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 05 personas, del Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional curso de administración de la solución adquirir, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica. Temas: ✓ Introducción de la solución adquirir ✓ Configurar la solución la solución adquirir tanto hardware y software - bypass ✓ Crear políticas para la protección del tráfico ✓ DNS protección ✓ Administración reporte en la consola ✓ Excepciones de políticas (Black & White lists)

	✓ Asignaciones de perfiles **Nota:** Se debe realizar laboratorios teóricos prácticos del temario.
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: <u>Líder o gerente del Proyecto:</u> Profesional responsable de coordinar y supervisar la ejecución del contrato, así como de comunicarse con el supervisor del contrato para garantizar el cumplimiento de los objetivos y las obligaciones establecidas, encargado de la implementación de 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 ✓ Especialista en gerencia de proyectos. <u>Implementación:</u> 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 tres (03) años. ✓ Deberá contar con las siguientes certificaciones: o Certificación o constancia de entrenamiento en la solución ofertada emitido por el fabricante o por un ente certificador autorizado por el fabricante. o Certificación de experiencia técnica en instalación y/o soporte de los productos de la plataforma DDoS e IPS ofertadas. ✓ Las certificaciones deben ser avaladas por el representante legal de la empresa y/o el jefe del Área de Seguridad o a quien le compete de la compañía donde se efectuaron las implementaciones; así mismo las certificaciones deberán acreditar mínimo dos años (02) de experiencia, debe acreditar al menos tres (3) certificaciones **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.. • 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 <u>Otras obligaciones del contratista:</u> 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.

El OFERENTE

_____

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